-

Los Pilares de la Seguridad Corporativa: presente y futuro

TRABAJO DE FINAL DE GRADO

UNIVERSIDAD DE BARCELONA

GRADO EN SEGURIDAD

Autor: Abel vazquez Gutiérrez

Tutora: Anna Aisa Biarnés

Junio 2018

La seguridad necesita aprender a funcionar en un entorno más complejo y con mayores expectativas y demandas, y al mismo tiempo, el trabajo se realizará en entornos de mayor riesgo y amenazas.

(Ljupcho, 2016)

DEDICATORIAS Y AGRADECIMIENTOS

Dedicatoria

A mi padre,

Sin duda alguna la persona que con menos palabras me ha enseñado más en la vida. Su capacidad de esfuerzo, honestidad y cariño, son sólo algunas de las virtudes que hacen de él un referente para mí. Hasta el último día peleaste como un campeón, sin dejar de sonreír a ese pequeñín que te quería tanto, tu nieto, mi hijo. Gracias

A mi hijo,

Con la esperanza que algún día seas capaz de perdonarme por el tiempo que no te he podido dedicar y con el deseo de haberte podido transmitir alguno de los valores que el abuelito me transmitió a mí. Perdón

A Cito,

Mi compañera de viaje, mi mujer, mi amiga, gracias por confiar ciegamente en mí, por estar siempre a mi lado, por hacer de padre y madre cuando yo no he podido estar. Gracias

Agradecimientos

A mi amigo Joan Carles Carbí i Blanch,

Gracias por todo lo que me has enseñado durante estos 4 años, por tu amistad, por tus consejos, por tu tiempo, por las horas al teléfono y en definitiva por aguantarme. Has puesto el listón muy alto, en lo personal y en lo profesional. Para mí el mejor activo de la primera promoción del grado. Sigue luchando como siempre haces, todo llegará, tendrás lo que te mereces …

A Anna Aisa Biarnés,

En una sociedad machista, en un sector como es el de la seguridad, hace que todo tu trabajo tenga aún más valor si cabe. Capacidad, conocimiento, esfuerzo, rigor y profesionalidad son valores que poca gente sabe combinar como tú con la humildad. Gracias por todo el tiempo que me has dedicado y por saber subirme la autoestima.

A todas las personas que he entrevistado para realizar este trabajo,

Agradeceros el tiempo, vuestra generosidad, por compartir conmigo vuestro conocimiento y por ayudarme a darme cuenta que en seguridad nunca se sabe suficiente o como alguno de vosotros dice, a que no tengo ni idea de seguridad, sólo un poco.

1. ÍNDICE

1. INTRODUCCIÓN

Allende la dimensión arquitectónica que se desprende del título escogido, huelga decir que el objeto de la presente investigación es ofrecer una herramienta objetiva que ayude a determinar cuáles deben ser las áreas de conocimiento mínimas que cualquier director de seguridad debería tener para ofrecer soluciones integrales de seguridad acordes a la visión panóptica que dicha responsabilidad le confiere. Asimismo, parecería razonable que la estructura funcional del departamento de seguridad corporativa fuera una réplica, a grandes rasgos y en la medida de lo posible, de dichas áreas de conocimiento que he bautizado como los pilares de la seguridad corporativa.

A tenor de lo que en el pasado reciente nos ha brindado la seguridad privada, existe una creencia más que arraigada en la sociedad española que pasa por asociar directamente, como si de un acto reflejo se tratara, la seguridad privada con el vigilante de seguridad y alguna que otra medida de seguridad adicional. Nada más lejos de la realidad, con sólo una somera aproximación a la parva normativa sectorial, se infiere que tal creencia es una interpretación deletérea del concepto de seguridad privada. Esta afirmación no es óbice para asumir que, efectivamente, la seguridad física es una de las actividades troncales de la seguridad privada y que por lo tanto se configura como uno de los pilares que la sustentan. No obstante lo dicho, se pretende analizar si sólo un pilar basta para aguantar la concepción de seguridad privada que la sociedad del presente y del futuro demandan o si bien necesita de más pilares para sustentarse.

La inmersión en el teatro de operaciones español en el periplo que va desde el año 1992 -año en el que entró en vigor la primera ley de seguridad privad- hasta la actualidad, servirá tanto para dar respuestas a las concepciones pretéritas del concepto de seguridad privada como para pergeñar su futuro inmediato.

La inclusión de la seguridad privada en el sistema de seguridad pública español ha determinado, en gran medida, cómo se ha ido gestando su relación a lo largo de la historia. La amalgama de recursos legislativos, desde la propia Constitución Española hasta las diferentes leyes sectoriales, tanto en materia de seguridad pública como en materia de seguridad privada, ha ido esbozando el modo en el que se ha concretado tal concomitancia, el resultado de la cual es uno

de los factores explicativos de la idiosincrasia de la seguridad privada tal y como la conocemos hoy.

Fue la primera ley en materia de seguridad privada, la Ley 23/1992 del 30 de abril, la que acuñó cómo debía establecerse tal relación. La seguridad privada quedaba subordinada a la seguridad pública. A efectos prácticos, esta subordinación se traducía en la necesidad de disponer de autorización previa para la creación de empresas de seguridad privada; la acreditación *ex ante* del personal de seguridad privada como condición *sine qua non* para poder ejercer; pero especialmente, al control *ex post* de la empresa de seguridad privada por parte de los cuerpos policiales y que se concreta en inspecciones y sanciones.

Tal relación explica, en buena parte, cómo ha evolucionado la seguridad privada. De hecho, no es descabellado inferir que, ante tal relación, la evolución de la seguridad privada ha bebido de la evolución de la seguridad pública. Esta última ha sufrido diversas mutaciones desde la transición española. De un modelo de orden público – en aras de evitar el desorden público- evolucionó a un modelo de seguridad ciudadana – para evitar la inseguridad ciudadana- hasta llegar al modelo de seguridad humana emanado el Programa de las Naciones Unidas para el Desarrollo en el año 1994 (Zigorraga, 2006), (González, 2014)

No obstante lo dicho, en el ínterin del año 1992 hasta la actualidad, ha habido otras variables que se han ido imbricado a tal relación y que han ido dibujando el panorama actual de la seguridad privada: las tendencias neoliberales de carácter anglosajón auspiciadas por la crisis del estado del bienestar; el descontento de muchas empresas de seguridad sobre la adecuación normativa; la globalización y los nuevos riegos que forman parte del ADN de las TIC así como la necesidad de ampliación de las competencias de la seguridad privada para reforzar la seguridad ciudadana. Estos factores fueron los precursores de la nueva ley de seguridad privada 5/2014 (Framis, 2014). Una ley que cojea, todo hay que decirlo, por no disponer de un reglamento que la desarrolle acorde con lo que se desprende de su contenido y denostada por el hecho de tener que ser interpretada conforme al reglamento que desarrolla la anterior ley y que data del año 1994.

El espíritu de esta nueva ley acrece –de iure- la posición del sector privado respecto la seguridad pública, dejando de poner énfasis en el principio de subordinación para pasar a desarrollar más eficazmente el principio de la complementariedad haciéndose valer de la cooperación y de la

corresponsabilidad. Este nuevo protagonismo del sector privado dibuja un nuevo escenario del sistema de seguridad donde tradicionalmente el sector público abrazaba más espacio. Mientras los servicios del sector privado han crecido exponencialmente, la parte pública, en cuanto a nuevas atribuciones, ha permanecido moderadamente estable. Esta nueva realidad acarrea intrínsecamente un cambio de rol en la relación de poder de la parte pública y privada, situando a esta última en una posición cada vez más consolidada y privilegiada fruto del protagonismo al que se hace referencia.

Antes de seguir avanzando en el tiempo, conviene analizar alguna de las epifanías de la subordinación de la seguridad privada a la seguridad pública ya comentada. De hecho, una de estas manifestaciones ha sido el principal estímulo de la presente investigación. Se trata de la presencia de ex miembros de las Fuerzas y Cuerpos de Seguridad del estado, -en adelante FCSE- ocupando los puestos de directores de seguridad corporativa de las principales empresas del territorio español. La mayoría de estos puestos se ha consolidado en una época de clara subordinación. Una época en la que parte del aparato policial -normalmente, aunque no necesariamente altos mandos- ha encontrado en lo privado un nicho de mercado para satisfacer sus intereses crematísticos, entre otros. Cabe analizar también si tal situación encuentra justificación, allende la mencionada relación de subordinación, en los modelos de seguridad pública de orden público y, especialmente, en el modelo de seguridad ciudadana que como ya he referido, han contagiado a un más que permeable modelo de seguridad privada. Un modelo que antaño ha sido capitalizado por la figura del vigilante de seguridad y por las medidas de seguridad. Cabe pensar que, ante tal concepción de la seguridad privada, las empresas optaran por hacer valer el *know how* de los miembros del entramado policial en esta materia y quien sabe si su red de contactos como principal acicate para integrarlos en sus plantillas.

Resultará interesante analizar si este criterio de elección ha aportado algún valor añadido a la empresa – que debe ser inherente en la figura del director de seguridad-, o más bien ha sido óbice para poder ofrecer al empresario soluciones de seguridad integral, de manera proactiva y no de manera reactiva *por mor del lack* de conocimiento. Convendrá ver también como han lidiado con los nuevos retos y amenazas no incluidos en la vasta temática que se enseña en las academias de policía del estado.

El carácter polimórfico que caracteriza la seguridad se ha acentuado durante los últimos años gracias a la globalización y al desarrollo de las tecnologías de la información. Esta combinación ha incorporado en nuestra sociedad nuevas amenazas y riesgos que necesitarán ser objeto de análisis por los profesionales de la seguridad. La sociedad ha llegado a un punto en el cual cualquiera de sus integrantes, ciudadanos, administración y persona jurídica, puede obtener y compartir por sus propios medios y de manera inmediata cualquier información, desde cualquier lugar y en la manera que desee (Claret, 2015). Es lo que conocemos como sociedad de la información, la cual confiere a la información la categoría del principal activo de las empresas y *por ende* el principal activo a proteger por los profesionales de la seguridad.

Tal desmán de información, obtenida principalmente a través de fuentes abiertas, hace que resulte complejo poder explotarla y poder desgranar aquélla realmente relevante para nuestros objetivos, o, si lo extrapolamos al sector empresarial, aquella información que hace a las empresas ser más competitivas frente al resto. Esta información no contempla tabú alguno. La red, el Internet 2.0, y la *Deep Web,* incorporan información relativa a todos los ámbitos de la sociedad, y el de la seguridad es uno de ellos. De esta forma, el espionaje tal y como lo conocíamos hasta ahora, ha mutado hacia una nueva realidad que nos ofrece el binomio formado por globalización y tecnologías de la información. Sigue vigente, no obstante, la marcialidad con la que estados, organizaciones e incluso los individuos se valen para obtener ventajas estratégicas, políticas y económicas; ha cambiado la herramienta pero no la finalidad.

Sin duda alguna, la información es el punto de partida de lo que hoy en día se conoce como inteligencia, y en el caso que nos compete, de la inteligencia estratégica. Gracias a ésta, su receptor se nutre de una herramienta que le permite anticiparse, disponer de un conocimiento especializado y de información elaborada que le posibilita tomar decisiones minimizando su riesgo (Escuela Superior de las Fuerzas Armadas *et al.*, 2016). Tan potente herramienta, ha sido exclusiva de los estados, *ub initio*, y sólo ha sido utilizada por el sector privado como inteligencia económica, reservando siempre lo relativo a seguridad al todo poderoso estado. La realidad actual nos brinda un escenario totalmente diferente. Un escenario en el que, tal y como se ha anticipado, la información de índole securitaria campa a sus anchas en forma de terabyte por las entrañas de Internet y que ha amplificado el espectro de las unidades de inteligencia al servicio de las empresas. Por si fuera poco, gracias a estas comunidades y al binomio tecnología y globalización, esta información traspasa las fronteras sin más óbice que el precio que permite

acceder a ella. Se trata de una concepción deletérea desde la óptica de los estados; una concepción *en ciernes* de ofrecernos un nuevo estado de la seguridad; una seguridad gaseosa –con el permiso de Z. Bauman- dado que la información se disipa por la red a pesar de los esfuerzos de los estados para contenerla en el interior de sus fronteras.

Se abre la veda para que las empresas privadas puedan incorporar inteligencia en el seno de sus departamentos de seguridad, permitiéndoles disponer de información privilegiada mucho antes que las Fuerzas y Cuerpos de Seguridad del estado. La especialización de las comunidades de inteligencia, y la superioridad de recursos económicos del sector privado sobrepasa la capacidad del estado y preconiza una nueva relación entre la seguridad pública y la seguridad privada, esta última encorsetada en gran parte por la primera.

La información no sólo hay que tratarla sino también hay que protegerla. Como se ha mencionado anteriormente, se trata de uno de los activos más valiosos de las empresas y, en consecuencia, objeto de amenazas y de ataques constantes que deberán ser debidamente tratados y, en su caso, contrarrestados. La ciberseguridad se ha abierto camino en el seno de las empresas como una de sus mayores preocupaciones. En este sentido, la ciberseguridad tiene como misión garantizar la integridad, disponibilidad, accesibilidad y confidencialidad de la información. Resulta paradójico que, en un mundo empachado de tecnología el conocimiento en materia de ciberseguridad sea tan escaso y, en consecuencia, sea temido por todo aquél que no sea profesional del sector. Este temor y desconocimiento son algunas de las variables que explican en buena medida que la ciberseguridad o seguridad informática se integre en los departamentos de sistemas y no en los departamentos de seguridad. Se infieren otros como el recelo de los departamentos de sistemas a las injerencias de departamentos ajenos.

1.1 Pregunta de investigación

Tras este somero análisis de la seguridad privada a lo largo de las últimas décadas y ante las nuevas y prolíficas amenazas dimanadas del binomio globalización y tecnología de la información, procede, sin más ambages, plantear la siguiente pregunta de investigación:

¿Cuáles son los pilares que deberían configurar la estructura de los departamentos de seguridad corporativa?

2. MARCO CONTEXTUAL Y TEÓRICO

El espectro de la investigación está limitado en tiempo por el ínterin que va desde el año 1992 hasta la actualidad y en espacio al territorio español. Del análisis del periplo mencionado se pretende inferir mediante un proceso de ilación, cuál será el escenario de la seguridad corporativa en un futuro a corto y medio plazo.

La pregunta planteada no ha sido objeto de estudio con anterioridad, motivo por el cual deberá ser abordada mediante la aproximación conceptual de las diferentes variables que abrazan el marco de estudio.

2.1 Seguridad privada, seguridad corporativa y seguridad integral.

El concepto de seguridad privada se ha ido ensanchando si tomamos como referencia la nimia definición que la primera ley española en la materia -la ley 23/1992- nos ofreció. Se trata de una visión encorsetada y naif de la seguridad privada que tiene como objeto la vigilancia y seguridad de personas y bienes por parte de personas privadas (Izquierdo Carrasco and Parejo Alfonso, 2004ª). Ante este enfoque paupérrimo, no es de extrañar, que diversos expertos, traigan a colación una retahíla de enfoques más ambiciosos. El concepto de seguridad privada adquiere la propiedad de supraconcepto en tanto en cuanto puede albergar la prevención del delito, la eventualidad de un incendio y otros aspectos relacionados con la seguridad económica o la protección de la privacidad (Barbero, 2001). Esta visión integra las nociones anglosajonas de Safety -protección de accidentes fortuito- y Security -protección y prevención de incidentes intencionados-. La seguridad privada responde a la tendencia de privatizar los espacios vitales, y obedece a la necesidad del sistema capitalista de proteger los beneficios particulares de las empresas (Bosch *et al.*, 2004).

Seguridad privada, seguridad corporativa y seguridad integral son conceptos que acostumbran a utilizarse indistinta e indiscriminadamente y que convendría precisar. Como se refería anteriormente, la ley de seguridad privada 23/1992, ofrecía una visión naif y carca del concepto de seguridad privada si tenemos en cuenta cómo se ha ido ensanchando su teatro de operaciones. Tal ensanchamiento hay que interpretarlo en su vertiente física – donde se diluyen las lindes entre la parte pública y la privada-, y también en una vertiente operacional, dada la asunción funcional con una clara tendencia *in crescendo*; una realidad *in fieri* a pesar del

hieratismo que respira la ley de seguridad en vigor, 5/2014, que define la seguridad privada como *"el conjunto de actividades, servicios, funciones y medidas de seguridad adoptadas, de forma voluntaria u obligatoria, por personas físicas o jurídicas, públicas o privadas, realizadas o prestados por empresas de seguridad, despachos de detectives privados y personal de seguridad privada para hacer frente a actos deliberados o riesgos accidentales, o para realizar averiguaciones sobre personas y bienes, con la finalidad de garantizar la seguridad de las personas, proteger su patrimonio y velar por el normal desarrollo de sus actividades."* Tal como se desprende del análisis realizado más adelante en el epígrafe "compendio normativo", el conjunto de actividades, servicios y medidas de seguridad ofrece una visión paupérrima y esquizofrénica -muy lejos de la realidad- que además se contradice – por su gran parecido en cuanto a atribuciones a la ley que le precede- con lo que se determina en la exposición de motivos -que apunta a tal ensanchamiento en otros términos-.

Dicho lo cual, dado que no existe ni definición ni doctrina al respecto de la seguridad corporativa, a renglón seguido se pretende realizar una aproximación conceptual, mediante un proceso de ilación, que permita sentar las bases sobre las cuales se pretenderán situar sus pilares básicos –desiderátum y leitmotiv de la presente investigación-.

Inobjetablemente, nos referimos a seguridad corporativa cuando queremos expresar la seguridad que se presta en el seno de la empresa –incluso en aquellas empresas de seguridad-. Cabrá entonces escudriñar cuáles son las actividades de seguridad que tienen lugar en el sí de una empresa. Huelga decir que, teniendo en cuenta la nimiedad de las actividades y servicios que nos blinda la ley, y para poder salvar tal escollo, se abordará el análisis desde la perspectiva de la figura del director de seguridad. Para ello la estrategia a seguir será, por un lado, examinar las funciones que le atribuye la ley, y por otro lado hociquear las corrientes anglosajonas respecto a esta figura.

2.1.1 La figura del director de seguridad, un comodín necesario.

Del contenido de los apartados b y c del artículo 36.1 de la LSP –analizados en el epígrafe de compendio normativo- se desprende que es función del director de seguridad: "*la identificación, análisis y evaluación de las situaciones de riesgo que puedan afectar a la vida e integridad de las personas y a su patrimonio así como la planificación y control de las actuaciones precisas para la implantación de medidas destinadas a prevenir, reducir y proteger la manifestación que riegos*

de cualquier naturaleza mediante la planificación y desarrollo de los planes de seguridad aplicables". El inmovilismo del legislador respecto a la evolución de iure del articulado por lo que respecta a las actividades y servicios en el ínterin del 1992 al 2014 –año de entrada en vigor de las leyes troncales de seguridad privada-, se ve contrarrestado por este halo de luz y esperanza que dimana de las atribuciones, en ciernes, de la figura del director de seguridad. Unas atribuciones que, como si de un relé se tratara, conectarán con la realidad que demanda el mercado.

La figura del director de seguridad actúa como una correa de transmisión que conduce a un nuevo paradigma de seguridad. Atrás queda la carcunda figura del director de seguridad con bigote y gafas de sol vigilando la puerta de la empresa. El nuevo perfil obedece a un perfil directivo conocedor del negocio y que integra los asuntos de seguridad con la toma de decisiones del conjunto de la empresa con el doble objetivo de, por un lado, la consecución de los objetivos de la empresa y, por el otro, ser capaz de obtener una ventaja competitiva para su empresa (Sánchez, 2007). Para lograr sus objetivos, el director de la seguridad debe conocer y comprender las amenazas, vulnerabilidades y riesgos de los activos corporativos. Tales riesgos deberán ser administrados de manera rentable, asegurando una capacidad mínima de inversión en los riegos aceptados (Ljupcho, 2016).

Esta realidad es igualmente percibida por el Instituto Nacional Estadounidense de estándares que le atribuye al director de seguridad – Chief Security Officer CSO- el rol de liderazgo para proporcionar una estrategia de seguridad integral para contribuir a la viabilidad y al éxito de la empresa para lo cual los más altos niveles orgánicos de las empresas (ANSI/ASIS CSO.1-2013 Chief Security Officer (CSO) Organizational Model, 2017).

Bajo este nuevo paradigma, se amplía el abanico funcional, competencial y relacional del director de seguridad corporativo en la actualidad (D'Antonio, 2018):

Esta visión de la figura del director de seguridad, contrasta con la visión tradicional. El hombre de bigote y gafas de sol, abandona la puerta de la empresa y accede a ella para ocupar una posición estratégica gozando de una perspectiva panóptica que le permita ayudar en la consecución de los objetivos de la organización.

Para dar respuesta a esta nueva exigencia que el mercado acarrea, no bastará con que el director de seguridad se afeite el bigote y se quite las gafas de sol. La responsabilidad intrínseca del nuevo rol, debería servir de acicate para que se replantearan cuestiones como los requisitos de formación que exige la ley para ocupar el cargo y, en la misma línea, considerar si la contratación de ex miembros de las FCSE conlleva algún valor añadido *per se,* para el desempeño del cargo –una realidad en el teatro de operaciones español-.

La seguridad corporativa, no sólo abraza medidas técnicas e implementaciones fruto del análisis de riesgo, sino que requiere además habilidades de gestión que coadyuven a la consecución de los intereses crematísticos de la organización, mediante la implantación de medidas efectivas y frugales para aquellos riesgos que deban ser contrarrestados y determinar aquellos riesgos que la corporación asume, sin menoscabar la actividad nuclear de la misma. En este sentido, la seguridad debe alinearse con el negocio, y para ello los directores de seguridad deben entender el *core business* de la organización y cómo contribuyen ellos a sus objetivos (Briggs, Edwards and Pickard, 2006).

Así pues, puede llegar a entenderse la seguridad corporativa como el conjunto de políticas, y procedimientos estratégico-operativos, encaminados a la gestión transversal de la seguridad en el sí de la empresa, implementando eficientemente medidas correctoras para aquellos riesgos inasumibles y determinando los riegos toreables cuya asunción no menoscabe la actividad nuclear de la organización.

2.1.2 La cultura de Seguridad, como binomio de la Seguridad integral

Otro de los conceptos que se utilizan indiscriminada e indistintamente es el de seguridad integral, del cual, la ley de seguridad privada 5/2014 se hace eco en su exposición de motivos como una de las razones de ser de la propia ley, atribuyéndola, a renglón seguido, a la nómina de responsabilidades del director de seguridad. A pesar de ello, el legislador no acota el concepto.

Tal inasibilidad ha conducido a diversos autores a bosquejar una aproximación conceptual del término seguridad integral. Un concepto que es un oxímoron en sí mismo dada, por un lado, la categoría polimórfica de la seguridad y por otro, la necesidad de encorsetar, delimitar y, en definitiva, abordar todos los aspectos y ámbitos de la seguridad.

En este sentido, la seguridad integral abraza una pluralidad de elementos e incorpora distintos aspectos de ámbitos físicos, jurídicos, científicos y técnicos yendo desde la higiene en el trabajo, a la seguridad pública y privada, seguridad informática, alimentaria, pasando por el análisis, la prevención y evaluación de riesgos. Desde esta perspectiva, se entiende seguridad integral como la seguridad en sentido amplio que interactúa con otros campos íntimamente vinculados –medio ambiente, calidad industrial y responsabilidad corporativa- (Gairín, 2011). Es interesante destacar de la definición la mención que hace al análisis de riesgos. Dicho análisis actúa como elemento disruptor de la seguridad integral.

Para la realización del análisis de riesgo, atribuido funcionalmente por la ley de seguridad privada a la figura del director de seguridad, se necesitan conocimientos en materia de seguridad de la suficiente magnitud como para conferirle una visión holística y panóptica – tal y como se comentaba en el epígrafe anterior- en concomitancia con el conocimiento de la organización, de su cultura y de su negocio.

Dependiendo del tipo de empresa, del sector, de su estrategia, de sus *stake holders* y, en definitiva, de una miríada de variables, el resultado del análisis será uno u otro y por lo tanto no se puede determinar un patrón de los elementos constitutivos de la seguridad integral. Dicho de otra forma, dependiendo de estas variables, el cuadro presentado anteriormente, contemplará más o menos elementos.

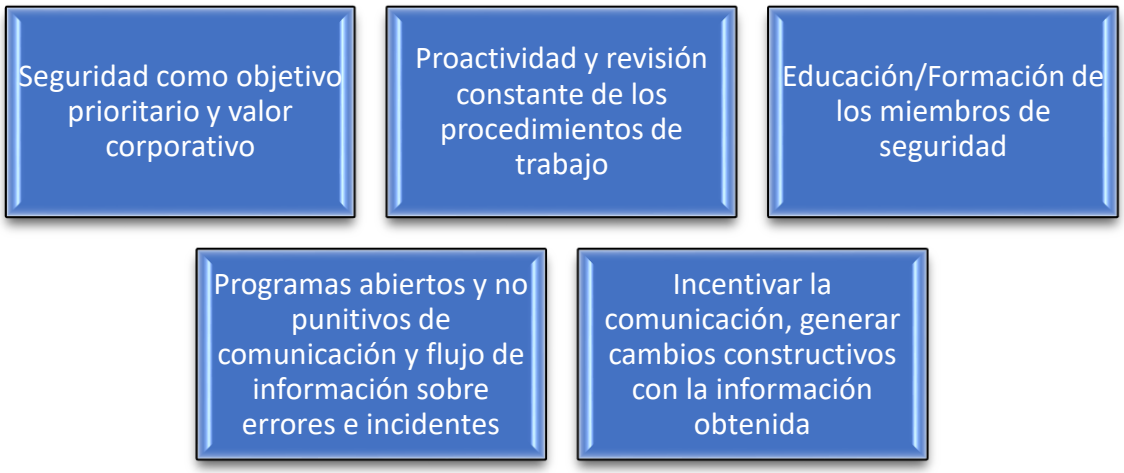
No obstante lo dicho, es importante señalar que la seguridad integral debe complementarse por la cultura de seguridad. A pesar por los esfuerzos de las organizaciones para asegurar sus sistemas y datos, siguen estando expuestos al riesgo ya que las personas no ven la seguridad como una prioridad y no son conscientes del riego que entrañan determinadas acciones (Swartz, 2005). De nada sirve tener una política acertada de antivirus si el usuario abre correos de dudosa procedencia o conecta dispositivos personales; de nada sirve implementar políticas de seguridad en los sistemas de información para acabar con la contraseña personal apuntada en un post-it enganchado al monitor; de nada sirve disponer de medidas contraincendios si mantenemos abierta con una cuña, la puerta encargada de asegurar un sector. Las entidades deben centrar su atención para diseñar políticas efectivas y motivar al individuo a seguir esas políticas. En definitiva, las organizaciones tienen que hacer frente al dilema de cómo promover políticas y procedimientos de seguridad para los empleados de la forma más efectiva posible (Dutta and McCrohan, 2002).

Por norma general, las organizaciones no quieren ver la realidad de su estado, la esconden o la minimizan. En este sentido una de las funciones claves del director de seguridad –que la ley no le otorga- es sensibilizar y orientar hacia una cultura de seguridad a todas las esferas de la organización, es decir, integrar la seguridad en toda la estructura empresarial (Sánchez, 2007). Para llevar a cabo tal misión, no sólo será suficiente su capacidad persuasiva, sino que, indefectiblemente, deberá ocupar una posición en el organigrama empresarial que le confiera el poder suficiente como para que su mensaje circule por todo el tejido organizativo sin encontrarse con ningún trombo que paralice tal cometido. Una de las primeras figuras indispensables a las cuales hay que hacer partícipe en primera instancia de la cultura de seguridad, es la del director general. Para ello, el director de seguridad, conocedor del negocio de la organización, deberá traducir un lenguaje securitario a un lenguaje económico o, dicho de otra manera, cómo afectan las amenazas fruto del análisis de riesgos a la consecución de los

objetivos de la organización. La comunicación entre ambas figuras debe ser fluida y directa, es decir, preferiblemente sin intermediarios que puedan distorsionar el mensaje.

Así pues, la creación de una cultura de seguridad es la estrategia más efectiva y sólida a largo plazo para la prevención en el seno de cualquier organización y se articula como condición *sine qua non* para alcanzar la seguridad integral. Una cultura de seguridad es, en esencia, una cultura en la cual las organizaciones, sus procesos y procedimientos de trabajo están orientados a mejorar la seguridad y donde todos sus profesionales están concienciados de manera constante y activa del riesgo que se produzcan errores, así como identificar su papel como sujeto que tiene que contribuir a evitar que se produzca el error, a comunicarlo y a aprender de él (Vásquez, 2016).

Las organizaciones con una cultura de seguridad sólida se caracterizan por:



(Vásquez, 2016).

2.2 Seguridad y sociedad de la información

La seguridad no se puede analizar de manera aislada, por si sola, al margen de la sociedad. Evoluciona al ritmo que ésta lo hace y adquiere un carácter dinámico que configura su génesis polimórfica. Se trata de una construcción social que va incorporando la suerte de riesgos y amenazas a los que la sociedad se va enfrentando. Por esta razón, por lo que respecta a la seguridad privada, el mercado ha dibujado un escenario totalmente distinto al del año 1992 y al que los profesionales del sector han tenido que adaptarse a una nueva era, la sociedad de la información.

A finales del SXX ya se empezaba a hablar de la sociedad de la información. Los expertos percibían los primeros indicios de transformación de la sociedad industrial a otro tipo de sociedad en la cual, los procesos de producción y optimización industrial quedaban relegados a un segundo plano, ocupando el primero el control y manejo de la información. Actualmente, las sociedades de la información "*se caracterizan por basarse en el conocimiento y en los esfuerzos por convertir la información en conocimiento. Cuanto mayor es la cantidad de información generada por una sociedad, mayor es la necesidad de convertirla en conocimiento. Otra dimensión de tales sociedades es la velocidad con la que la información se genera, se transmite y se procesa. En la actualidad la información puede obtenerse de manera prácticamente instantánea y, muchas veces, a partir de la misma fuente que la produce, sin distinción de lugar*" (Linares López and Ortiz Chaparro, 1995:114). La revolución de las comunicaciones y la proliferación de la información en Internet, han supuesto un incremento considerable de la información hasta entonces inaccesible o – siendo más rigurosos-, sólo hasta entonces accesible por el estado.

2.3 La herramienta: inteligencia estratégica

Por lo tanto, la información está al alcance de todos. Todo lo que nos rodea es información a la cual podemos acceder de forma rápida, inmediata y sencilla. Cabrá preguntarse si toda esa información es útil o, dicho de otra manera, qué es relevante dentro de tal barahúnda de datos. La respuesta a tal interrogante trae a colación la inteligencia. El proceso de conversión de la información a inteligencia es la actividad troncal de lo que se conoce como inteligencia estratégica. No obstante, encontrar una definición de inteligencia que se ajuste a todas las corrientes científicas no ha sido posible hasta la fecha. Y es que como apuntaba el filósofo español Jaime Balmes (SXIX) "*Sólo la inteligencia se examina a sí misma*".

Los autores que a lo largo de la historia han intentado encontrar una definición que recoja aquello esencial que tiene que tener la inteligencia se pueden englobar en dos grandes corrientes. La primera de ellas abraza a los autores con un perfil estrictamente académico como pueden ser Sherman Kent i Willmoore Kendall, protagonistas del conocido debate Kent-Kendall. La obra de Kent fue la primera exposición teórica de lo que hoy se conoce como inteligencia moderna (Taplin, 1989). El segundo grupo se extiende a aquellos autores que han tenido cierto bagaje de campo, que han sido profesionales de la inteligencia desde un punto de vista práctico

y operativo. Dentro de este grupo se encuentran Winn L. Taplin y Ehihelm Agrell y su paradigma responde al lema *"La inteligencia una cubierta elegante para el espionaje poco elegante*" (Troy, 1991). Ambos grupos han intentado ofrecer una definición inclusiva que diese respuesta a tal paradigma, cada uno desde su óptica y desde su propia experiencia. Como siempre, cuando hay más de una explicación para una cosa es que tal cosa no está clara: La inteligencia de finales del SXIX no tiene nada que ver con el espionaje de los *practiseners* de la segunda mitad de SXX ni tampoco con las demandas de las unidades de inteligencia de la actualidad. Intentar dar una definición inclusiva es una "Misión Imposible" que ni el mismo Tom Cruise, en el mejor de sus papeles, con sus mejores gadgets y con la mejor compañía sería capaz de abordar. No obstante, las diferentes escuelas encuentran puntos de convergencia en el sentido de la inteligencia en sí misma, en su finalidad. Para nuestro objeto de estudio es más que suficiente. De esta manera, lo primero que debemos considerar es que inteligencia e información no son lo mismo. El proceso de producción de inteligencia requiere un método que permita tratar la formación de forma eficiente para poder aportar un conocimiento veraz y exacto a su destinatario final. No sólo permite anticiparse a acontecimientos, sino que también aporta conocimiento riguroso y especializado que permite a su destinario la toma de decisiones asumiendo el menor riesgo posible. (Escuela Superior de las Fuerzas Armadas *et al.*, 2016).

Dadas las características de la sociedad de la información, los servicios de inteligencia han mutado respecto sus orígenes. Como epifanía a lo mencionado, la concepción de la inteligencia como espionaje forma parte del pasado, *por mor de* que el origen de la información de nuestra sociedad actual, lo encontramos a través de fuentes abiertas OSINT – *Open Source Inteligence*- a través, principalmente, de la red. La globalización fue el nudo gordiano que condujo a la liberación de la inteligencia de las garras de los estados. Por un lado, ha servido para generar unas relaciones de interdependencia estatales y la aparición de entes supraestatales desconocidos hasta la fecha. Por otro lado, ha hecho posible la entrada en escena de actores privados que hasta el momento no habían tenido protagonismo en este mundo. Esta nueva realidad ha hecho convulsionar las estructuras de las agencias de inteligencia que no han tenido otro remedio que adaptarse para poder atender esta nueva demanda: "*Las nuevas demandas y los nuevos objetivos han puesto de manifiesto la obsolescencia -eso sí, no programada- de las bases de datos de los servicios de inteligencia"* (Rathmell, 2002:94). La globalización no sólo ha permitido la incorporación de nuevos actores privados, sino que muchos de ellos ocupen hoy en

día una posición privilegiada respecto a los estados. El sector privado encuentra en la inteligencia la herramienta necesaria para situar su empresa en una situación de ventaja respecto al resto de empresas competidoras.

Asimismo, la globalización y las tecnologías de la información han contribuido a la aparición de las comunidades de inteligencia. Se trata de un sistema integrado por agencias y organismos en materia de inteligencia coordinados por una estructura con una función específica. Tal coordinación es compleja por el poder que el manejo y control de la información trae consigo inherente: injerencias en las competencias propias de cada uno de los actores; escasez de interés en compartir información y dificultad en los procesos de coordinación horizontal. Las comunidades de Inteligencia pueden ser consideradas sistemas, es decir, un conjunto de inteligencia y de información relacionados entre sí, ordenados y con un objetivo en común. Como todo sistema, su eficiencia no debe ser medida como la suma de las partes por separado. Es un valor añadido respecto a la mencionada suma (Escuela Superior de las Fuerzas Armadas *et al.*, 2016).

En la empresa, el valor de la inteligencia se asocia con la capacidad que ofrece para reforzar aquellas decisiones necesarias para afrontar su futuro. Se trata de un cambio disruptivo de las organizaciones privadas a la hora de enfocar sus estrategias, un cambio necesario para la gestión de las organizaciones. De este modo, el futuro de la inteligencia estratégica en el sector privado está ligado al modo en que sea capaz de servir a las necesidades estratégicas del decisor. Se augura que en el ámbito privado, y dada su importancia, la inteligencia estratégica pase de las manos del responsable de seguridad a la mesa del presidente de la CEO (Fournier *et al.*, 2015).

2.4 Ciberespacio, una dimensión en forma de amenaza

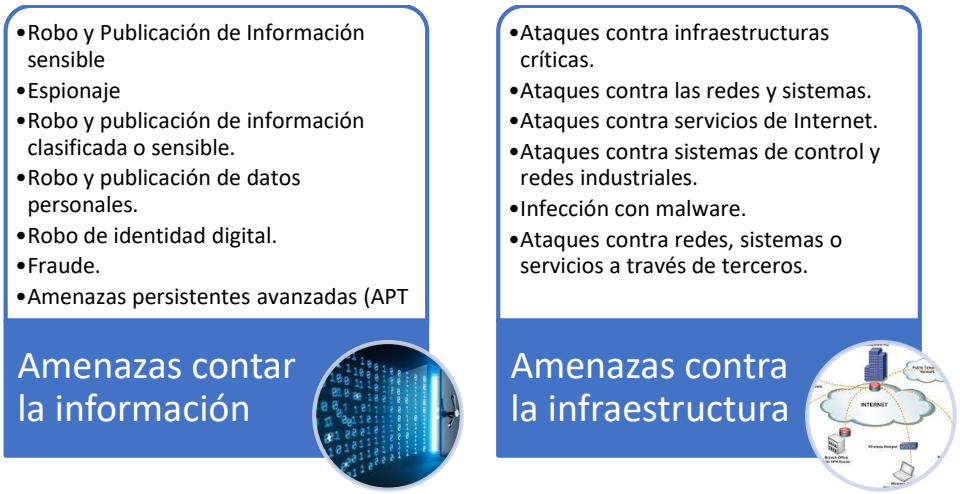
Nada tienen que ver – en términos relativos- las amenazas y los riesgos societarios que inspiraron al legislador a elaborar la primera ley de seguridad privada, con la pléyade de riesgos y amenazas inherentes al binomio formado por las tecnologías de la información y la globalización. Ante esta nueva situación, los profesionales de la seguridad deben conocer cuáles son las principales amenazas, las principales vulnerabilidades y de qué medios disponen para su paliación. La respuesta a todos estos aspectos nos permite afirmar que la nueva generación de riesgos y amenazas tiene por objeto nuestros cibersistemas dado el elenco de información que en ellos se alberga. Toda nueva amenaza comporta nuevos atacantes. La tecnología ofrece la posibilidad de guardar el anonimato y de atacar desde cualquier lugar del mundo con lo que la miscelánea de transgresores se eleva exponencialmente: servicios y agencias de información, delincuentes, terroristas, intrusos y simples competidores (Fournier *et al.*, 2015). Ha sido la tecnología la que ha abierto una dimensión adicional desdibujando las fronteras tradicionales y abriendo un debate acerca de las responsabilidades del estado; de esta manera, el ciberespacio se articula como el conjunto de medidas y de procedimientos basados en la tecnología de la información y la comunicación, configurados para la prestación de servicios (Fojoz *et al.*, 2012), (Fernández and Rodríguez, 2017).

El *"Global Risk Report 2017"* no escapa a esta realidad. De hecho, dedica un epígrafe entero para dar cuenta de la magnitud de las amenazas de esta nueva generación. Las tecnologías emergentes de la cuarta revolución industrial (4RI) han incorporado cambios substanciales que afectan transversalmente a la sociedad. Añade además que la profunda interconexión entre los riesgos mundiales, sus interdependencias y la velocidad con la que se fraguan los cambios, hacen que las transiciones tecnológicas tengan un efecto multiplicador del riesgo (World Economic Forum, 2017)

Las amenazas en el espacio adquieren una dimensión global que va más allá de la propia tecnología. En los últimos años, ha aumentado considerablemente tanto la intensidad como el grado de sofisticación de los ataques. Los estados tienen que blindarse y proteger sus intereses ante grupos subversivos que aprovechan el anonimato que les ofrece la tecnología para perpetrar sus ataques. El robo de información, los ataques ransomware, ataques de denegación de servicio, el hackeo de dispositivos móviles y los ciberataques contra las infraestructuras críticas capitalizan las principales amenazas del ciberespacio (Seguridad Nacional, 2017).

La ciberseguridad ha venido para quedarse, y ha evolucionado de tal manera que de proteger la información reactivamente aplicando medidas correctoras *ex post*, ha pasado a la anticipación, a trabajar en un plano preventivo, para lo cual los planes director y la implantación del Sistema de Gestión de la Seguridad de la Información (SGI) apoyado en los estándares ISO vigentes son las principales herramientas. En el pasado la ciberseguridad respondía a la prioridad de proteger la información -*Information Security-,* amenazada principalmente por accesos o usos ilegítimos, revelación de secretos, fallos de disponibilidad, alteración y destrucción. Esta tendencia ha evolucionado hacia la gestión de riesgos del ciberespacio – Information Assurance- que se basa en el análisis y la gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de datos y los sistemas y procesos usados basándose en los estándares de información (Fojoz *et al.*, 2012).

Las dos grandes categorías en las que se engloban las principales amenazas en el plano cibernético son las amenazas contra la información y las amenazas contra la infraestructura TIC.



Fuete Instituto Español de Ciberseguridad (SCSI)

El ciberespacio no supone solamente nuevas amenazas. Esta nueva dimensión permite a los delincuentes explotar una vía adicional a las existentes, con las ventajas ya mencionadas. El terrorismo yihadista ha encontrado en Internet y Internet 2.0 un comburente perfecto para hacer llegar su discurso a todo el mundo, una herramienta fundamental en sus estrategias de captación y radicalización (Garriga Guitart, 2015).

La mayoría de grandes empresas españolas cuentan con una estructura interna que implementa políticas y medidas englobadas en el marco de la seguridad de la información. No obstante, la situación cambia radicalmente en el caso de las pequeñas y medianas empresas que suponen un 99% del tejido empresarial, donde la falta de recursos económicos para invertir en seguridad o en formación o la falta de conocimiento y concienciación tienen como resultado la falta de implantación de medidas de seguridad. Así pues, es necesario formar y sensibilizar a todos los usuarios de la organización, incluyendo todos los niveles para que tomen conciencia y actúen en consecuencia. (Fojoz *et al.*, 2012).

La proliferación de dispositivos móviles, Smartphone y tabletas supone otro vector de amenaza que ensancha el ecosistema del riesgo dado que se han incorporado a procesos corporativos en los que habitualmente se trata información sensible, motivo por el cual los profesionales de la seguridad deben implementar medidas encaminadas a proteger tal información.

Es primordial disponer de una política de seguridad corporativa que implemente una batería de restricciones a los usuarios siguiendo las recomendaciones ISO, así como a la migración de servicios a la nube o la utilización incluso de dispositivos propiedad del usuario BYOD – *Bring your own device*-. Para ello, es necesario que la dirección acepte la existencia de riesgos y promueva políticas de seguridad dentro de la organización.

No obstante, las empresas no sólo son víctimas de los ciberataques, también son verdugos. La explicación de este doble rol se debe a que las organizaciones privadas, empujadas por su afán de incrementar su cuenta de resultados, son las protagonistas de muchos de los ataques que se perpetran en la red; ataques dirigidos a sus competidores y que tienen como finalidad hacerse con su información. Se trata de ciber espionaje industrial. Otro modo de conseguir información, de manera subrepticia pasa por utilizar las aplicaciones o servicios que venden a sus clientes para obtener toda la información personal posible y ponerla a la venta en el mercado sin el consentimiento de los usuarios (Fojoz *et al.*, 2012).

3. HIPÓTESIS

Dada la pregunta de investigación se plantean las siguientes hipótesis como aproximación a lo que, a criterio del investigador, podrían ser respuestas al problema planteado. No obstante, deberán ser debidamente analizadas, validadas y refutadas desde la perspectiva holística que nos confiere el propio proceso de investigación.

La inteligencia estratégica y la ciberseguridad se configuran como las principales herramientas de la seguridad corporativa para la gestión del riesgo y amenazas del presente y del futuro.

- Hipótesis deductiva

La falta de formación en materia de ciberseguridad es uno de los factores principales por el cual la ciberseguridad se estructura dentro de los departamentos de sistemas.

- Hipótesis inductiva

La formación exigida por ley a los directores de seguridad no facilita la gestión integral de la seguridad de una manera preventiva. Los aboca a una respuesta reactiva ante las nuevas amenazas.

- Hipótesis inductiva

Las unidades de inteligencia en el seno de los departamentos de seguridad corporativa se consolidan como la principal herramienta para trabajar en el plano preventivo.

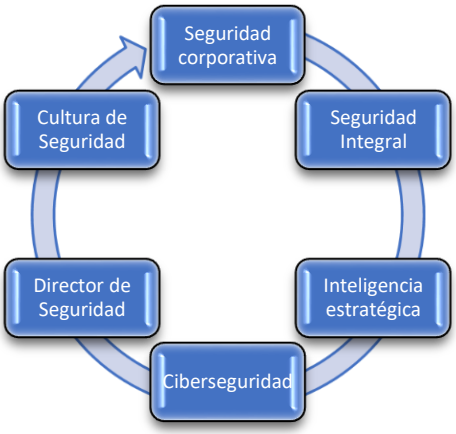
- Hipótesis deductiva

El acceso a la inteligencia en el área de seguridad corporativa, situará la balanza a favor de la seguridad privada dentro de la tradicional relación entre ésta y la seguridad pública

- Hipótesis inductiva

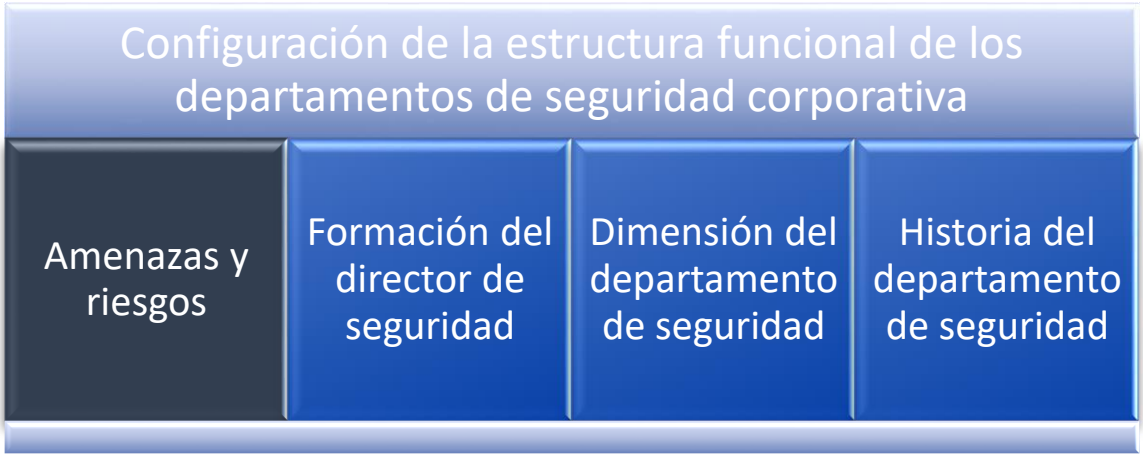
4. CONCEPTOS CLAVE

La propia concepción analítica conceptual del marco teórico nos da una aproximación precisa a los conceptos que, a criterio del investigador, deberían quedar claros para la correcta comprensión de la investigación planteada.



5. VARIABLES

Alrededor de la cuestión planteada giran diversos factores que pueden influir en la medida que adoptan distintos valores. Como variable dependiente, derivada de la cuestión planteada, se determina la siguiente: "Configuración de la estructura funcional de los departamentos de seguridad corporativa". El resto de variables planteadas son consideradas independientes ya que un cambio en su valor afecta a la variable principal. Entre ellas la variable "amenazas y riesgos" se articula, a priori, como la de más entidad. No obstante, a criterio del investigador, el resto de variables enumeradas deben ser tenidas en cuenta puesto que también condicionan la variable dependiente.



6. METODOLOGÍA

6.1 Entrevistas

La técnica de investigación es, en esencia, cualitativa pese a que serán tenidos en cuenta y como objeto de análisis documental informes y estadísticas que contemplan técnicas cuantitativas. Ante la escasa ciencia que existe respecto la pregunta planteada, con un marco teórico de naturaleza analítica conceptual prácticamente en su totalidad, la investigación se apoyará principalmente en entrevistas y análisis documental para completar la parte empírico explicativa y poder hacer así inferencias causales que respondan a la pregunta de investigación.

Para ello, la estrategia escogida para el diseño muestral, pasa por realizar entrevistas en profundidad a ocho directores de seguridad. Es importante señalar que el perfil, formación,

procedencia y ámbitos profesionales de los directores de seguridad entrevistados es distinto siendo uno de ellos una infraestructura crítica. Adicionalmente, para complementar y contrastar el resultado de esta suerte de entrevistas, se entrevistarán a las siguientes personas:

1. Experto reconocido en ciberseguridad a nivel nacional e internacional: la entrevista será enfocada para extraer aquella información relativa a su experiencia en la empresa privada. Principales amenazas que trata, en qué departamento se ubica la ciberseguridad y por qué, el nivel de conocimiento percibido en la materia y nivel de implementación de las medidas de seguridad.
2. Experta reconocida en identidad digital: principales demandas por parte de las empresas. Cuál es su relación con los departamentos de seguridad. Nivel de conocimiento percibido en su materia. Gestión de seguridad por parte de las empresas en lo que respecta a la identidad digital.
3. Experto reconocido en inteligencia estratégica: obtener información de cuáles son sus principales demandas por parte de las empresas. Cómo valora el nivel de formación en su materia por parte de los departamentos de seguridad. Qué aporta la inteligencia a las empresas, principalmente en el área de seguridad.

6.2 Análisis documental

El hecho de que no haya una definición con base científica del concepto de seguridad corporativa, es sólo un botón de muestra de la menesterosa e inasible ciencia existente en lo que respecta al núcleo de la investigación. Tal realidad conduce por un lado a adoptar estrategias de aproximación exploratorias, que se estriban, en buena medida, en un profuso análisis documental y por otro lado sirve de estímulo para el investigador.

6.2.1 Compendio normativo

A lo largo del siguiente epígrafe, se analizará parte del elenco normativo en materia de seguridad privada en España haciendo a su vez referencia a otra normativa relacionada con el objetivo de urdir una línea argumental que coadyuve a dar respuesta a la pregunta de investigación y también para lograr entender cómo interaccionan las variables de estudio en las hipótesis planteadas.

El núcleo del análisis normativo para comprender la realidad actual girará en torno a la Ley de Seguridad Privada 5/2014, en adelante LSP. No obstante, y por aquello de que todo hecho presente encuentra una justificación pretérita, se analizará también, aunque de forma somera, la primera ley de seguridad privada post-constitucional y el reglamento que la desarrolla. Me refiero a le ley 23/1992 de seguridad privada y al reglamento 2364/1994, un reglamento con ligeros *upgrades* en forma de órdenes ministeriales, que complementa también la actual LSP, carente de uno a medida; en definitiva, toda una entropía dentro del rimero legislativo.

Tal análisis, en el ínterin desde el año 1992 hasta la actualidad, será de gran valor para hacernos una idea de la concepción de seguridad privada que el legislador ha querido desarrollar. No obstante lo cual, el hecho que la LSP no disponga, a fecha de hoy, de un reglamento *ex profeso* es motivo de entidad suficiente como para inferir que no es de interés del legislador cambiar sustancialmente la mayoría de aspectos en materia de seguridad privada, a pesar de los esfuerzos inherentes a todo el proceso que acarrea la entrada en vigor de una nueva Ley. Se trata de una situación que contraviene la realidad del sector privado, que demanda un cambio de paradigma en materia de seguridad privada, que avance de forma síncrona con la realidad social y que no sea óbice para satisfacer sus intereses crematísticos que se ven amenazados por la incerteza que emana del hieratismo legislativo. Una demanda que, a su vez, se ve acrecentada por la falta de recursos para abastecer la demanda de reposición de los cuerpos policiales que vislumbra, con la aquiescencia de éstos, una distorsión en la linde funcional entre seguridad pública y privada que la miscelánea legislativa se ha preocupado tanto y, en cierta medida con un trasfondo draconiano, de preservar (Palomar Olmeda and Álvarez Moreno, 2014).

6.2.1.1 La relación entre la seguridad pública y la seguridad privada: ver, oír e informar

En epígrafes anteriores se ha hecho referencia a la relación entre la seguridad pública, y la seguridad privada, a cómo se ha ido gestando, cómo ha ido fraguando e incluso si tal relación puede ser una variable que justifique la capitalización de los ex miembros de las FCSE en los puestos de los directores de seguridad. El germen de tal relación obedece, en buena medida, al artículo 149.1.29 de la CE que establece como competencia exclusiva del estado la "*Seguridad pública, sin perjuicio de la posibilidad de creación de policías por las Comunidades Autónomas en la forma que se establezca en los respectivos Estatutos en el marco de lo que disponga una ley orgánica*" estableciendo así, una barrera entre ambas seguridades, difícilmente franqueable, *de iure.* Una barrera que el propio Tribunal Constitucional trae a colación en diversas sentencias

como la STC 154/2005 y la STC 33/1982 en la que se concluye que la seguridad privada es "*la prestación por personas, físicas o jurídicas, privadas de servicio de vigilancia y seguridad de personas o bienes, que tendrán la consideración de actividades complementarias y subordinadas respecto a las de la seguridad pública*" (Palomar Olmeda and Álvarez Moreno, 2014). Es importante referir que una sentencia que data con fecha anterior a la ley 23/1992 establecía, allende la definición de seguridad privada, la relación de subordinación que aún hoy en día se mantiene vigente, a pesar de los esfuerzos por maquillarlo de la LSP vigente.

La complejidad conceptual y competencial a la que se ha hecho referencia, se ve acrecentada aún más con la entrada en escena de la seguridad ciudadana y el orden público. Tal vez, como atajo nemotécnico, pensar en el antónimo de estos últimos nos ayude a comprender su significado, aunque aun así, cuesta establecer el límite entre unos y otros términos.

Tal y como señala Manuel Izquierdo (Izquierdo Carrasco and Parejo Alfonso, 2004b) la jurisprudencia del Tribunal Constitucional conduce a señalar que la seguridad pública está dirigida a la protección de personas y bienes , mantenimiento de la tranquilidad y orden ciudadano y que las actividades de las FCSE no agotan su ámbito material – el de la seguridad pública-.

Por si no fuera suficientemente complejo, cabe señalar que el análisis del contenido de las actividades de seguridad privada que el art. 5 de la LSP recoge, y que será objeto de análisis a posteriori, pone de manifiesto la subsunción de dichas actividades con la jurisprudencia constitucional correspondiente a la conceptualización de la seguridad pública. Tal concomitancia conduce inexorablemente a la inclusión de ciertas actividades de seguridad privada a lo que la propia ley determina que es seguridad pública. Se trata de una evidencia que no debería sorprendernos si fuéramos lo suficientemente responsables como para entender de qué va esto de la seguridad, que es cosa de todos y que todos sumamos.

La estrategia del legislador para lidiar con esta palmaria distorsión funcional se ha traducido en determinar cuál es la relación orgánica y las reglas del juego del binomio seguridad pública y seguridad privada. El articulado 23 /1992 hacía referencia, ya en su preámbulo a lo siguiente: "*En este marco se inscribe la presente Ley, en su consideración de los servicios privados de seguridad como servicios complementarios y subordinados respecto a los de la seguridad pública*".

Veintidós años más tarde, el teatro de operaciones de la seguridad privada ha ido *in crescendo*. Similar al efecto bola de nieve, las empresas de seguridad privada han ido ensanchando sus fronteras físicas en detrimento de la seguridad pública. Tal circunstancia abre una ventana de oportunidad a la seguridad pública que le permite centrar sus recursos en el ámbito de la seguridad ciudadana, ofreciendo así soluciones y respuestas más acrisoladas.

La linde funcional aún es más borrosa, si cabe. La tecnología, así como la cuenta de resultados en términos de eficacia y eficiencia de la seguridad privada explican, en buena parte, esta realidad. Más importante resulta aún señalar que esta realidad no ha pasado inadvertida por el legislador que, tal y como se desprende de su preámbulo, ha sido uno de los estímulos de la LSP. El resultado es nuevamente una actitud tuitiva respecto la seguridad pública; eso sí, cuidando más las formas, pero olvidando el fondo. La nueva ley de seguridad privada 5/2014 configura la nueva relación ya en su preámbulo: *" La ley pasa de poner el acento en el principio de la subordinación a desarrollar más eficazmente el principio de complementariedad a través de otros que lo desarrollan, como los de cooperación o de corresponsabilidad, mediante una técnica legislativa más flexible que permite una adaptación permanente a los cambios que experimente la sociedad sin que sea precisa una reforma de rango legal para ello."*

Una afirmación que contrasta con esta otra que realiza a renglón seguido: "A partir de ahí, se establece un conjunto de controles e intervenciones administrativas que condicionan el ejercicio de las actividades de seguridad por los particulares. Ello significa que las Fuerzas y Cuerpos de Seguridad han de estar permanentemente presentes en el desarrollo de las actividades privadas de seguridad, conociendo la información trascendente para la seguridad pública que en las mismas se genera y actuando con protagonismo indiscutible, siempre que tales actividades detecten el acaecimiento de hechos delictivos o que puedan afectar a la seguridad ciudadana".

Nuevamente, la declaración de intenciones es, cuanto menos confusa, *por mor* de tanta contradicción. Entender entonces de qué va esto de la subordinación requerirá de un ejercicio de *snorkel* a lo largo del articulado. Del título V de la LSP dimanan las actividades de control, inspección, y medidas provisionales completadas por las de sanción en el título VI. El artículo – art 53. In fine- atribuye estas funciones a las Fuerzas y Cuerpos de Seguridad del Estado. Por otro lado, el artículo 27.3 faculta al Cuerpo de Policía Nacional y a la Guardia Civil, dependiendo de los casos, para la habilitación del personal de seguridad privada. En definitiva, una serie de

imposiciones administrativas que ponen de manifiesto la subordinación de la seguridad privada respecto a la seguridad pública. Una subordinación que no sólo contempla aspectos administrativos sino de carácter más operacional, cuando ambas seguridades coliden en espacio, tiempo en el ejercicio de las mismas funciones. En tal caso el personal de seguridad privada queda sometido al de seguridad pública tal y como se desprende del artículo 8 de la LSP y su remisión al artículo 30.

Una de las grandes novedades que presenta la LSP y que pretende ofrecer mayor protección jurídica al personal de seguridad privada es el artículo 31 de dicha ley que, bajo circunstancias muy concretas la misma protección jurídica que a los agentes de la autoridad. Nuevamente, la formulación de tal precepto es confusa y en cierto modo subjetiva. Más allá de analizar la concepción del vigilante de seguridad como agente de la autoridad, interesa señalar el matiz de subordinación que se infiere de la lectura del articulado puesto que condiciona la categoría de agente de la autoridad a aquellas situaciones en las que el vigilante, debidamente identificado, siendo víctima de desobediencia y agresión, se encuentre en cooperación y bajo el mando de las FCSE.

Una vez visto el principio de subordinación, es menester abordar a qué se refiere el legislador cuando introduce los términos colaboración y coordinación; dos conceptos que acostumbran a ir de la mano pero que merecen ser analizados por separado.

El artículo 8 de la LSP habla por sí solo: "De conformidad con lo dispuesto en la legislación de fuerzas y cuerpos de seguridad, las empresas de seguridad, los despachos de detectives y el personal de seguridad privada tendrán especial obligación de auxiliar y colaborar, en todo momento, con aquéllas en el ejercicio de sus funciones, de prestarles su colaboración y de seguir sus instrucciones, en relación con los servicios que presten que afecten a la seguridad pública o al ámbito de sus competencias."

Tal afirmación menoscaba nuevamente la posición de la seguridad privada dado que se desprende que tal vinculación no se da en sentido contrario, un flaco favor para el interés general y un *craso error* de enorme magnitud en una situación de alerta terrorista de nivel 4 sobre 5, de riegos tecnológicos y de amenazas híbridas en la que el intercambio de información resulta vital. No obstante, el artículo 14 amplía el concepto de colaboración y abre un haz de esperanza: "*Las Fuerzas y Cuerpos de Seguridad podrán facilitar al personal de seguridad*

privada, en el ejercicio de sus funciones, informaciones que faciliten su evaluación de riesgos y consiguiente implementación de medidas de protección. Si estas informaciones contuvieran datos de carácter personal sólo podrán facilitarse en caso de peligro real para la seguridad pública o para evitar la comisión de infracciones penales".

A todo esto, el reglamento 2364/1994, en su artículo 66, se hace eco de esta colaboración con una visión más próxima a la concepción de subordinación propia de la ley 23/1992. Sin ánimo de reproducir el articulado – eso es harina de otro costal- su contenido es similar al artículo 8 de la LSP.

En cuanto a la coordinación, pergeñada ya en la ley 23/1992 y encarnada en las comisiones de coordinación desarrolladas en el reglamento 2364/1994, la nueva LSP trata este concepto en su artículo 16, sin aportar cambios sustanciales respecto a la normativa anterior. Por lo que respecta estrictamente a la coordinación sigue apostando por la fórmula de las comisiones mixtas, desarrolladas en la Orden INT/315/2011 en cuyo artículo 4 se recogen las funciones y que, a groso modo, pasan por asesorar al Ministerio de Interior, proponer criterios de homogeneización, intercambiar experiencias e información en materia de seguridad. Nuevamente la declaración de intenciones se queda en *agua de borrajas* dado que en la práctica estas comisiones, todo y que están constituidas, apenas se convocan.

A pesar de ello, cabe destacar los mecanismos de coordinación que distintos cuerpos policiales han creado persiguiendo los objetivos a los que el artículo 4 de la Orden INT/315/2011 hace referencia. A modo de ejemplo, encontramos RED AZUL en Policía Nacional, el programa COOPERA de la Guardia CIVIL y la "*Xarxa de Col·laboració*" de Mossos d'Esquadra.

Sin duda alguna, la gran novedad que incorpora la LSP por lo que respecta a la relación entre la seguridad pública y privada es la adición de la complementariedad como forma de relación. De hecho, el objeto de la ley así lo estipula en su artículo 1.2 "*Asimismo, esta ley, en beneficio de la seguridad pública, establece el marco para la más eficiente coordinación de los servicios de seguridad privada con los de las Fuerzas y Cuerpos de Seguridad, de los que son complementarios"*. A bote pronto, resulta esperanzador el contenido de tal artículo, pero, nada más triste de la realidad, haciendo un análisis global de todo el contenido de dicha ley, uno se da cuenta que tal complementariedad es un espejismo y que tal concepto debe ser concebido desde un prisma de subordinación. En este sentido, resulta muy interesante la reflexión que

plantea (Izquierdo Carrasco and Parejo Alfonso, 2004ª:95) que viene a concluir que tal novedad obedece a un intento a la desesperada de " *salvar el escollo del monopolio estatal de los servicios de seguridad y de no enturbiar los lazos con las Fuerzas y Cuerpos de Seguridad".* Tal conclusión tiene su origen en una nueva contradicción del legislador en la exposición de motivos de la LSP. Por un lado, atribuye la seguridad en exclusiva al monopolio del Estado para reconocer a posteriori que se han extendido actividades de seguridad por parte de otros agentes sociales o privados, en la línea del efecto bola de nieve comentado anteriormente. Todo un Oxímoron fruto del exceso de celo traducido en una ambigüedad que degenera en una inseguridad jurídica.

En definitiva, por lo que respecta a tal relación: ver, oír e informar.

6.2.1.2 Actividades, servicios y medidas de la nueva LSP

Parece del todo razonable que, haciendo una inmersión en el compendio legislativo por lo que respecta a las funciones que realiza el personal de seguridad privada – actividades y servicios para ser puristas-, obtendremos una pista del abanico funcional que reserva el legislador al personal de seguridad privada que a su vez servirá para vislumbrar su noción conceptual al respecto de la seguridad integral.

Sin lugar a dudas, la tecnología ha transformado la forma en que se concibe la sociedad, su binomio, la globalización, aún han ahondado más en la profundidad de los cambios. El uso masivo de tal tecnología ha ensanchado el ecosistema delictivo, no tanto por la aparición de nuevos delitos sino por la evolución –gracias a esta tecnología- de los ya existentes. Del timo de la estampita hemos pasado al famoso "pishing", del robo con fuerza, hemos pasado a la intrusión en los sistemas de la información. Salvando las distancias, se trata del "mismo perro con distinto collar". No se pretende referir con esto, ni mucho menos, que unos delitos han sido sustituidos por otros, en absoluto, se trata de la incardinación de nuevos delitos a un nuevo ecosistema.

Como se ha mencionado en el epígrafe anterior, esta realidad, no ha pasado inadvertida por el legislador, el cual, ha elucubrado nuevas formas –de iure- para relacionarse con los agentes privados persiguiendo un doble objetivo. Por un lado, asegurarse el control que ya tenía de la seguridad privada, y por el otro, recogiendo toda aquella información de interés.

Otro de los actos reflejos del legislador y que también ha sido acicate para la entrada en vigor la LSP ha sido, precisamente, intentar reordenar y recoger las actividades y servicios de seguridad

privada. Los nuevos cambios tecnológicos han sido en gran parte precursores de tal necesidad, tal y como se desprende de la exposición de motivos de la LSP "*Otros dos factores determinantes de la necesidad de sustituir la vigente ley cabecera de este sector del ordenamiento jurídico son los importantísimos cambios tecnológicos, que condicionan la prestación de servicios de seguridad, y la tendencia a la integración de las distintas seguridades en un concepto de seguridad integral, cuestión a tener en cuenta tanto en el ámbito de las actividades como en el de las funciones y servicios que presta el personal de seguridad privada, aspectos éstos que la Ley 23/1992, de 30 de julio, no podía contemplar*".

Por primera vez, la LSP recoge el concepto de seguridad integral, un concepto que no amplía en la retahíla de artículos pero que asocia con la figura del director de seguridad. Una curiosa relación que será objeto de análisis en otros epígrafes.

La reformulación funcional inducida por los cambios tecnológicos obedece también a una de las grandes lacras con la que se han ido encontrando las empresas de seguridad privada: la intrusión de otros agentes privados en el sector.

Si más ambages, el contenido del artículo 5 de la LSP determina cuáles son las actividades de seguridad privada, es decir, aquellas actividades que únicamente pueden llevar a cabo las empresas de seguridad privada – con la salvedad del apartado "h" que es propia y exclusiva de los despachos de detectives- y que además limita las actividades a las que pueden dedicarse.:

> a) La vigilancia y protección de bienes, establecimientos, lugares y eventos, tanto públicos como privados, así como de las personas que pudieran encontrarse en los mismos

Dicho artículo incorpora dos novedades respecto al articulado anterior. Por un lado, se hace referencia a espacios públicos y por el otro a la protección de personas que pudiere haber en su interior.

> b) El acompañamiento, defensa y protección de personas físicas determinadas, incluidas las que ostenten la condición legal de autoridad.

Como principales novedades respecto a la ley 23/1992 añade las funciones de acompañamiento y defensa y por otro lado abre la puerta a que personal privado pueda ejercer la protección de personalidades con la condición de autoridad.

> c) El depósito, custodia, recuento y clasificación de monedas y billetes, títulos-valores, joyas, metales preciosos, antigüedades, obras de arte u otros objetos que, por su valor económico, histórico o cultural, y expectativas que generen, puedan requerir vigilancia y protección especial.

No se observan cambios substanciales respecto al articulado anterior.

> d) El depósito y custodia de explosivos, armas, cartuchería metálica, sustancias, materias, mercancías y cualesquiera objetos que por su peligrosidad precisen de vigilancia y protección especial.

Tampoco se observan cambios substanciales respecto al articulado anterior.

> e) El transporte y distribución de los objetos a que se refieren los dos párrafos anteriores..

A diferencia del articulado anterior, no hace referencia a los medios móviles con los que realizar tal función. Al margen de esta salvedad, no hay cambios sustanciales.

> f) La instalación y mantenimiento de aparatos, equipos, dispositivos y sistemas de seguridad conectados a centrales receptoras de alarmas o a centros de control o de videovigilancia.

Prácticamente igual al articulado anterior precisando aquellos aparatos, relativos a la seguridad que pudieren estar conectados a centrales receptoras de alarmas.

> g) La explotación de centrales para la conexión, recepción, verificación y, en su caso, respuesta y transmisión de las señales de alarma, así como la monitorización de cualesquiera señales de dispositivos auxiliares para la seguridad de personas, de bienes muebles o inmuebles o de cumplimiento de medidas impuestas, y la comunicación a las Fuerzas y Cuerpos de Seguridad competentes en estos casos.

A diferencia de la ley 23/1992, se abre la puerta a la monitorización de cualquier dispositivo de seguridad de las personas, de bienes o de inmuebles.

> h) La investigación privada en relación a personas, hechos o delitos sólo perseguibles a instancia de parte.

Tales funciones se subsumen con el contenido del artículo 19 de la ley ya derogada.

El análisis menesteroso realizado obedece a una estrategia con doble intencionalidad. Por un lado, pone de manifiesto que después de la declaración de intenciones en la que se hacía referencia a la necesidad imperiosa de modificar el compendio legislativo dados los avances tecnológicos –dedicando toda una liturgia dedicada a ello- la realidad es bien diferente. Las actividades de la nueva ley, son en esencia las mismas que las que ya incorporaba la ley 23/1992. Tal realidad conduce a hacernos una idea de la actividad nuclear de la seguridad privada. Una actividad que no evoluciona –de iure- y que pasa por una concepción tradicionalista de la seguridad.

Las actividades descritas en el artículo 5 de la LSP se complementan con lo que el legislador denomina como actividades compatibles y que luego desarrolla en el artículo 6. Tal artículo es la respuesta a una demanda del sector que no procede analizar para el objeto de investigación y que a nuestros efectos sólo es de interés por el contenido de su apartado 6: "*A las empresas, sean o no de seguridad privada, que se dediquen a las actividades de seguridad informática, entendida como el conjunto de medidas encaminadas a proteger los sistemas de información a fin de garantizar la confidencialidad, disponibilidad e integridad de la misma o del servicio que aquéllos prestan, por su incidencia directa en la seguridad de las entidades públicas y privadas, se les podrán imponer reglamentariamente requisitos específicos para garantizar la calidad de los servicios que presten*". El artículo cojeará a la espera de un reglamento que aborde la cuestión

de manera más amplia. Se trata de una coletilla que, desde el espectro de seguridad integral, en pleno siglo XXI, en plena sociedad de la información, debería situarse en el artículo que le precede y, por lo tanto, pasar a ser una de las actividades nucleares de los servicios de seguridad privada.

Analizadas las actividades de seguridad privada, el siguiente alto lo haremos en el capítulo II de la LSP, donde se detallan los servicios de seguridad que, de alguna manera, vienen a referir las acciones para llevar a cabo dichas actividades.

El artículo 40 establece aquellos servicios a prestar con arma de fuego, sin relevancia para el objeto de la investigación y enmarcado en una concepción física de la seguridad.

El siguiente artículo, viene a completar el artículo 5.1 de la LSP que amplía el campo de actuación físico de tal actividad obedeciendo a una demanda palmaria que pasa por la necesidad del sector privado por prestar servicios, en determinadas circunstancias, en espacios que, hasta el momento, se reservaban a las FCSE. Dicho lo cual, se trata nuevamente de una funcionalidad físico-tradicional al igual que el resto de servicios a los que la ley hace referencia a lo largo de todo el capítulo e incluso en el capítulo siguiente reservado a los servicios de los despachos de detectives.

Visto el carácter continuista y tradicionalista que ofrecen las actividades y medidas de seguridad, quedará analizar las medidas de seguridad privada que la ley contempla. No obstante, huelga decir que previo a la LSP, la ley 23/1992 hacía una remisión reglamentaria por lo que respecta al desarrollo de tales medidas. Así pues, el reglamento 2364/1994 hace referencia a las medidas se seguridad para aquellos establecimientos que requieran de transporte de monedas, billetes y otros objetos de valor, la obligación de disponer de armeros para aquellos emplazamientos donde se realicen servicios con armas de fuego, así como otras medidas de seguridad para establecimientos como entidades de crédito, joyerías, platerías, oficinas de farmacia, loterías y establecimientos de juego, entre otros.

Se trata, nuevamente de medidas físicas en las que se regulan, en gran parte todos aquellos aspectos técnicos, con el objetivo de que dispongan determinadas homologaciones o estándares UNE o UNE- EN.

Por lo que respecta a la LSP es en el artículo 51 donde tiene lugar el desarrollo normativo. A pesar de ello, es en el artículo 52 donde se establecen el tipo de medidas para la protección tanto de bienes como de personas. Clasifica las medidas en: medidas de seguridad física, de seguridad electrónica, de seguridad informática, de seguridad organizativa y de seguridad personal. Las dos primeras se corresponden con una visión tradicional de seguridad física, en la que se contemplan barreras para impedir acceso, así como mecanismos de prevención, detección de intrusión y alarmas.

La gran novedad es la inclusión de medidas informáticas, todo y que prácticamente reproduce el contenido del artículo 6.6 comentado anteriormente. El artículo 52.1 establece las medidas de seguridad informática de la siguiente manera :"*[..], cuyo objeto es la protección y salvaguarda de la integridad, confidencialidad y disponibilidad de los sistemas de información y comunicación, y de la información en ellos contenida*". Un contenido nimio, que, hasta la llegada del nuevo reglamento deberá ser interpretado de la manera más generalista posible.

Es importante señalar el contenido del articulado cuando hace referencia a las medidas de carácter organizativo: "[..] *dirigidas a evitar o poner término a cualquier tipo de amenaza, peligro o ataque deliberado, mediante la disposición, programación o planificación de cometidos, funciones o tareas formalizadas o ejecutadas por personas; tales como la creación, existencia y funcionamiento de departamentos de seguridad o la elaboración y aplicación de todo tipo de planes de seguridad, así como cualesquiera otras de similar naturaleza que puedan adoptarse*". La interpretación de este artículo ayuda a alejarnos de la concepción tradicionalista de seguridad privada y trae a colación otros aspectos como planificación, planes de seguridad, análisis de riesgo para hacer frente a cualquier tipo de amenaza, propios de la concepción contemporánea de la seguridad privada. En definitiva, un clavo ardiendo al que agarrarse para poder abrazar el concepto de seguridad corporativa y una visión más integral de lo que el legislador nos tiene acostumbrados.

6.2.1.3 La figura del director de seguridad

Más allá de las atribuciones que la LSP otorga al director de seguridad, es importante señalar que se trata de la figura que lidera la seguridad en el sí de una empresa. Por lo tanto, tanto el abanico funcional que el compendio legislativo le atribuye como la formación exigida para la habilitación de su cargo, serán de gran ayuda, aunque no por sí solo suficientes, para determinar

cuáles son los pilares de la seguridad en el seno de la empresa, así como para realizar una aproximación conceptual a la seguridad corporativa.

La ley vincula la existencia de la figura del director de seguridad a los siguientes condicionantes: que así lo exija la normativa de desarrollo de la LSP por el dimensionamiento del servicio; cuando se acuerde por decisión gobernativa o cuando lo prevea una disposición especial (art. 36.2 LSP). El homólogo del director de seguridad en una empresa de seguridad es referido por la LSP como la figura del jefe de seguridad. No obstante, la investigación sólo se centrará en la figura del director de seguridad.

Sin más dilaciones, se detallan las funciones que el art. 36 de la LSP le asigna a tal figura:

a) La organización, dirección, inspección y administración de los servicios y recursos de seguridad privada disponibles.
b) La identificación, análisis y evaluación de situaciones de riesgo que puedan afectar a la vida e integridad de las personas y al patrimonio.
c) La planificación, organización y control de las actuaciones precisas para la implantación de las medidas conducentes a prevenir, proteger y reducir la manifestación de riesgos de cualquier naturaleza con medios y medidas precisas, mediante la elaboración y desarrollo de los planes de seguridad aplicables.
d) El control del funcionamiento y mantenimiento de los sistemas de seguridad privada.
e) La validación provisional, hasta la comprobación, en su caso, por parte de la Administración, de las medidas de seguridad en lo referente a su adecuación a la normativa de seguridad privada.
f) La comprobación de que los sistemas de seguridad privada instalados y las empresas de seguridad privada contratadas, cumplen con las exigencias de homologación de los organismos competentes.
g) La comunicación a las Fuerzas y Cuerpos de Seguridad competentes de las circunstancias o informaciones relevantes para la seguridad ciudadana, así como de los hechos delictivos de los que tenga conocimiento en el ejercicio de sus funciones.
h) La interlocución y enlace con la Administración, especialmente con las Fuerzas y Cuerpos de Seguridad, respecto de la función de seguridad integral de la entidad, empresa o

grupo empresarial que les tenga contratados, en relación con el cumplimiento normativo sobre gestión de todo tipo de riesgos.

i) Las comprobaciones de los aspectos necesarios sobre el personal que, por el ejercicio de las funciones encomendadas, precise acceder a áreas o informaciones, para garantizar la protección efectiva de su entidad, empresa o grupo empresarial.

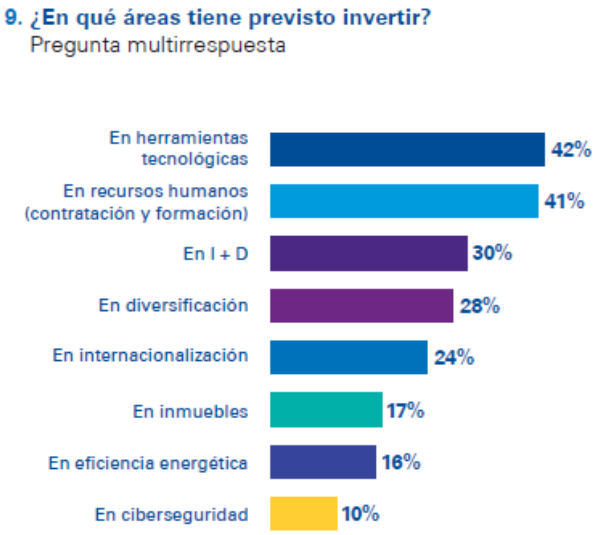
Se vislumbran ciertas atribuciones que escapan de la visión tradicionalista de la concepción de la seguridad privada e incluso de las actividades y servicios de seguridad a los que la LSP hace referencia. Los apartados a,b y c del artículo, en la línea de lo que ya se apuntaba en las medidas organizativas, atribuye una serie de tareas de gestión que pasan por la identificación, evaluación y el análisis del riesgo de cualquier naturaleza y a la planificación y organización en materia de seguridad para la implantación de medidas correctoras. Se infiere entonces que el director de seguridad deberá contemplar en su análisis de riesgo cualquier amenaza a los activos de las empresas, sea de la naturaleza que sea. Su visión de la seguridad deberá ser holística e integral, dado el carácter polimórfico-intrínseco que la caracteriza. Se infiere también que deberá dotarse de las herramientas necesarias –de acuerdo a la legislación- para hacer frente al resto de amenazas.

En relación a su formación, el artículo 29.d de la LSP establece que: “Para los jefes y directores de seguridad, en la obtención bien de un título universitario oficial de grado en el ámbito de la seguridad que acredite la adquisición de las competencias que se determinen, o bien del título del curso de dirección de seguridad, reconocido por el Ministerio del Interior” (Ministerio del Interior, 2014).

Por su parte, el Ministerio del Interior determina que para la habilitación de los directores de seguridad se deberán cumplir uno de los siguientes requisitos: el ya mencionado artículo 29.d o la acreditación del desempeño durante cinco años de puestos de dirección o gestión de seguridad pública o privada y superar las pruebas sobre las materias a las que se refiere el artículo 12 de la Orden INT/318/2011: “*tendrán carácter teórico-práctico y versarán sobre la normativa reguladora de la seguridad privada y, en especial, sobre servicios de seguridad, funciones de los departamentos de seguridad, y características y funcionamiento de los sistemas y medidas de seguridad*”.

La distancia que existe tanto entre la exigencia naif del artículo 12 de la de INT/318/2011, centrada básicamente en la experiencia, como en los requisitos exigidos en las habilitaciones de director de seguridad obtenidas con fecha anterior a la entrada en vigor de esta normativa, con respecto a las nuevas amenazas a las que se tiene que enfrentar un director de seguridad, pone de manifiesto la dificultad para ofrecer soluciones integrales y centralizar las políticas de seguridad en los departamentos de seguridad corporativa.

6.2.2 Ciberdelincuencia: el coste de la amenaza



(Arias,2017)

(Arias,2017)

En epígrafes anteriores se ha hecho referencia al impacto que las nuevas tecnologías han tenido en la sociedad. La implementación de la tecnología en la amalgama de procesos de ámbito empresarial adquiere una razón de ser un tanto Darwinista. Las empresas se tienen que adaptar a un mercado cada vez más competitivo que exige aumentar su productividad.

Al mismo tiempo que la tecnología hace fuerte al tejido empresarial, lo hace más vulnerable. Sin duda alguna, la Ciberseguridad se ha convertido en una de las amenazas que más preocupan a los empresarios. Las gráficas contiguas, rebelan los resultados de un estudio de la consultora KPMG sobre el sector de la PYMES en España durante el año 2016 (Arias, 2017). La información que nos ofrecen se complementa: vemos como por un lado como el 10 % de las

empresas prevén invertir en Ciberseguridad y por otro lado se observa como la ciberseguridad y la protección de la información es una de las principales amenazas para las PYMES -la primera en cuanto a seguridad-. Esta tendencia se ha ratificado e incrementado durante el resto de ejercicios. La explicación obedece al incremento tanto del número de amenazas como su potencial destructivo (Dreyer *et al.*, 2018). Los últimos episodios de las infecciones del WannaCry durante el 2017 afectaron a más de 3.000.000 ordenadores de 150 países mientras que el malware NotPetya causó sólo en un trimestre pérdidas por un valor de 300 millones de dólares americanos ('Global Risk Report 2018', 2018). Durante el año 2017 se lanzaron 357 millones de nuevas variantes de malware, una cifra que se espera que aumente durante los próximos ejercicios debido, entre otras cosas, al aumento desorbitado del número de dispositivos objeto de ser amenazados. Se prevé que de los 8,4 mil millones de dispositivos pasemos a los 20,4 mil millones en tan sólo dos años. El Global Risk Report en su edición 2018 rebela, mediante un estudio realizado durante el 2017 en 254 empresas de diferentes países, que el coste destinado a responder a los ataques cibernéticos ha sido un 27,4 % superior al del 2016 y la tendencia es a seguir en esta línea. Dato que concuerda con el vaticinio que realiza Cybersecurity Ventures, situando el coste a nivel mundial en 6 trillones de dólares en el 20121. Por otra parte, dicho informe señalaba la preponderancia existente a atacar cada vez más infraestructuras críticas.

Un estudio realizado en cerca de 36.000 empresas americanas, rebelaba que el 91 % habían sufrido en pérdidas de algún tipo debido a ataque informáticos y el 11,7 % de ellas había tenido que hacer frente a pérdidas económicas por encima de los 100.000 USD. En el continente americano, las pérdidas por este tipo de ataques se cuantifican en billones de dólares, afectando de forma más perjudicial a las pequeñas empresas y provocando, en alguna ocasión, a su quiebra (Balan *et al.*, 2017).

Esta nueva normalidad – como algunos hacen referencia- ha intentado ser cuantificada por numerosos informes. Se establecen diversas técnicas y variables de cálculo que dificultan comparar los resultados. A pesar de ello, todas concluyen en la prominencia en número y daño de los ataques cibernéticos – 62% de 2012 a 2017- y a la dificultad de realizar los cálculos, en gran parte, por la tendencia de las empresas a esconder debajo de la alfombra la información relativa a los ataques que han sufrido.

El portal web OpendataSecurity publicaba diversos informes en la línea de lo expuesto anteriormente (Arana, 2017) . La aseguradora británica Lloyd's conjuntamente con la empresa de seguridad informática Cyence concluían un estudio en el que reflejaban que las pérdidas producidas por Ciberataques en Estados unidos – 121.000 millones de dólares americanos- superaba las pérdidas ocasionadas por el Huracán Katrina -108.000 Millones de dólares americanos.-. Otra investigación determinaba que las empresas se gastan una media de 2 millones de dólares en hacer frente al malware y 2,4 millones de dólares debido a ataques Web. Los informes señalaban que el sector más afectado por los ataques es el financiero, cuyo coste medio anual se establece en 18,28 millones de dólares. En otro de los informes de la consultora Accenture se recalcaba el hecho de que el tamaño de la empresa y el número de conexiones a internet es directamente proporcional a los costes en sufragar los ataques.

El panorama europeo no escapa de esta realidad. ENISA determina que, durante el ejercicio del 2016, el coste de los incidentes de ciberseguridad puede llegar a suponer el 1,6 del PIB del país, siendo el sector financiero, el energético y el de las propias TIC donde se registran los costes más elevados y en todos los casos, el activo más atacado ha sido los datos.

El teatro de operaciones español es un reflejo de lo acontecido en el mundo. Durante el año 2016 las empresas españolas invirtieron 3,2 millones de euros para ciberblindarse pero aun así sufrieron pérdidas por un valor de 1,7 millones de euros debido a los ataques de los que fueron víctimas -malware y randsomware principalmente- (Mediana, 2017).

Los dos primeros meses del 2018 se han registrado más incidentes de seguridad en infraestructuras críticas que en todo el 2014 -125 frente 63- (elEconomista.es, 2018a). La compañía Norton estima que un 34,8 % de la población ha sido víctima de ataques on-line, generando 1.750 millones en pérdidas (65,52€ por persona y 22,1 horas en tiempo). El 56% de las víctimas sufrieron un ataque vía malware y el 39% fueron víctimas de pishing (Conversia, 2018).

6.2.3 El gobierno de la amenaza: odisea SXXI

6.2.3.1 Directiva NIS

A tenor de los hechos referenciados en el epígrafe anterior, organismos, organizaciones internacionales y gobiernos han desarrollado diversas iniciativas con el objetivo de urdir estrategias para tratar de paliar las amenazas intrínsecas del nuevo ecosistema. La Directiva

Europea 2016/1148 establece una serie de medidas homogéneas destinadas a garantizar unos estándares de seguridad en las redes y sistemas de la información. La Directiva NIS "Network Information Security" señala la importancia de disponer de unos sistemas seguros y estables en un entorno productivo tecno dependiente. El legislador pretende poner orden dentro de un ecosistema donde la entropía aumenta inenarrablemente. Por un lado insta a los estados a trabajar en la cooperación y por otro recalca la importancia que los actores - administraciones, empresas de servicios, tejido empresarial- adopten las medidas oportunas para la gestión del riesgo asociado a los ciberataques y a notificar a las autoridades nacionales competentes los incidentes que se produzcan dentro de este ámbito (Marzo, 2017). La Directiva ha sido la precursora para la implantación de iniciativas como los CSIRT - equipos de respuesta a emergencias informáticas- que sumado a las agencias de Ciberseguridad como ENISA – agencia europea- e INCIBE – agencia de ciberseguridad española- configuran todo un cordón sanitario para trabajar en la prevención y en la respuesta a la hemorragia de amenazas. El legislador establece que los estados miembros deberán:

- Adoptar una estrategia nacional sobre la seguridad de redes y sistemas de información.
- Crear un grupo de cooperación estratégica e intercambio de información entre los Estados miembros.
- Crear una red de Equipos de Respuesta a Incidentes de Seguridad Informática (red CSIRT), para contribuir en la rapidez y eficacia de la cooperación operativa.
- Establecer y notificar los requisitos de seguridad para operadores de servicios esenciales y proveedores de servicios digitales.
- Determinar obligaciones para las autoridades nacionales competentes de cada Estado miembro, de los puntos de contacto únicos y los CSIRT, en las tareas relacionadas con la seguridad de redes y sistemas de información.

('DIRECTIVA (UE) 2016/ 1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO', 2016)

Por su parte, el Ministerio del Interior no sólo suscribe lo anterior, sino que también establece una serie de recomendaciones adicionales a las empresas. En este sentido se reconoce la importancia que la dirección de las empresas acepte la existencia de riesgos y promueva políticas de seguridad dentro de la organización. Señala además la necesidad de fomentar una

cultura de la seguridad en el seno del tejido empresarial, acorde a la magnitud de las ciberamenazas (Instituto Español de Estudios Estratégicos, 2016).

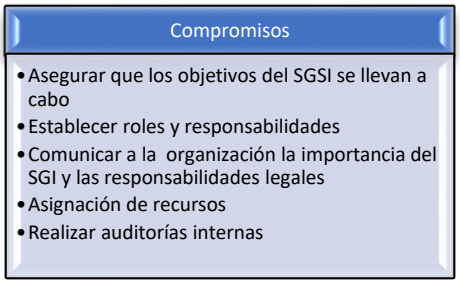
6.2.3.2 Estándares ISO

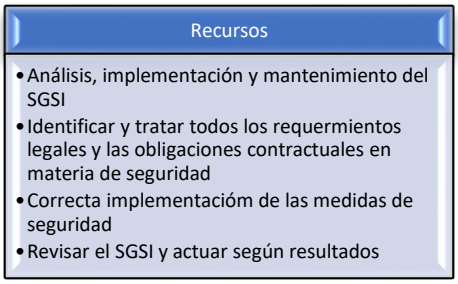
Se ha visto como a través de la directiva NIS se apunta a la necesidad de gestionar las amenazas y establecer estrategias de colaboración por parte de los estados y del tejido empresarial para tratar de neutralizarlas. Interesa, para el objeto de investigación, conocer cómo se debe llevar a cabo el liderazgo en materia de ciberseguridad, si existe una figura responsable para tal efecto y, en caso de que no exista, tratar de discernir, atendiendo al contenido objeto de análisis, a qué figura le compete tal liderazgo.

6.2.3.2.1 ISO 27001

La norma ISO 27001 se centra en el sistema de gestión de la seguridad de la información, en adelante SGSI. El objetivo de implantar un SGSI no es otro que garantizar que los riegos de la seguridad de la información sean conocidos, gestionados, minimizados o asumidos por toda la organización de forma estructurada, documentada, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías (ISO27001, 2005).

La norma señala que una correcta implementación del SGSI requiere la implicación de la dirección. Tal condición encuentra su razón de ser en el hecho de que el SGSI afecta a la gestión del negocio y, por lo tanto, de él se desprenden acciones y decisiones que sólo pueden emanar de la dirección de la corporación. El SGSI tiene una vertiente técnica – la implantación de medidas- y otra de gestión del riesgo que afecta a toda la compañía. En este sentido, la norma ISO traza una serie de compromisos señalando directamente a la dirección.





6.2.3.2.2 ISO 27002

La Norma ISO 27002 establece que las actividades de la seguridad de la información deberán coordinarse por representantes de diferentes departamentos de la organización de perfil

medio-alto. Amplía este concepto determinando que dicha coordinación pasa por involucrar a usuarios, diseñadores de las aplicaciones, gerentes, auditores e incluso personal de seguridad. Tal coordinación debe conducir a:

- Subsunción de las actividades de seguridad con las políticas de seguridad de la información.
- Aprobar metodologías y procesos para la seguridad de la información teniendo en cuenta la evaluación del riesgo.
- Evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información.
- Promover la cultura de seguridad.
- Monitorizar la información y determinar las acciones a emprender para dar respuesta a los incidentes detectados.

La norma apunta a la posibilidad de delegar en la figura de un gerente de seguridad de la información la responsabilidad integral en esta materia. Es importante señalar a su vez que la norma recomienda que las acciones de implementación y las políticas y controles deben realizarse de forma independiente con el objetivo de asegurar la idoneidad, eficiencia y eficacia de la organización para manejar la seguridad de la información. De la misma manera y con el mismo argumento, establece que la auditoría de los sistemas de la información deberá ser llevada a cabo por departamentos u otros actores externos ajenos a los departamentos encargados de la implantación de las medidas. Asimismo, señala la necesidad de establecer procedimientos en los que se determine bajo qué circunstancias y a qué autoridades se deberán reportar los incidentes de seguridad de la información.

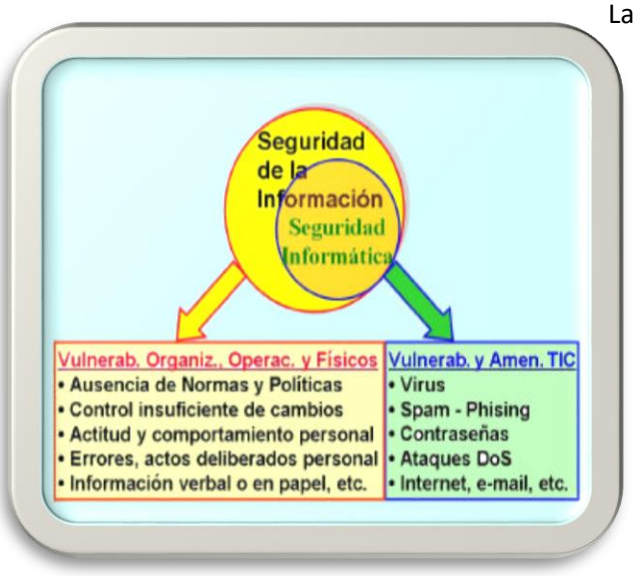
6.2.3.2.3 ISO 27014

La norma 27014 ofrece, en lo que respecta a la separación de poderes vislumbrada en la norma IS 27002, una visión un tanto más draconiana con el objetico de acrisolar la gobernanza de la seguridad de la información.

El concepto de seguridad de la información, ha ido mutando a lo largo de los años. De esta manera la seguridad de la información ha pasado de lo técnico – seguridad informática- a la gestión hasta institucionalizarse bajo normas universales. Actualmente la seguridad forma parte de los negocios dado que la información – el petróleo del SXXI- es un activo crítico

importantísimo para el devenir de las compañías, entroncándose así en el paradigma del *Corporice Gobernante* (Meyer, 2014). Dicho paradigma obedece a la necesidad de alinear la seguridad de la información con la estrategia de la propia empresa, permitiendo de esta manera conseguir una gestión de la seguridad de la información eficaz e invertir en seguridad de la información de una forma más efectiva.

La evolución de la seguridad de la información a la que se ha hecho referencia y que tiene sus orígenes en la seguridad informática, justifica el que la norma determine la necesidad de separar el gobierno de la seguridad informática del gobierno de la seguridad de la información. Sólo se prevé interacción en la convergencia entre el gobierno de la seguridad de la información y el gobierno de las TIC. Llama la atención que dicha circunstancia dista mucho del panorama del tramado empresarial español donde la gestión de la ciberseguridad se aborda, en la mayoría de los casos, desde el departamento de IT.

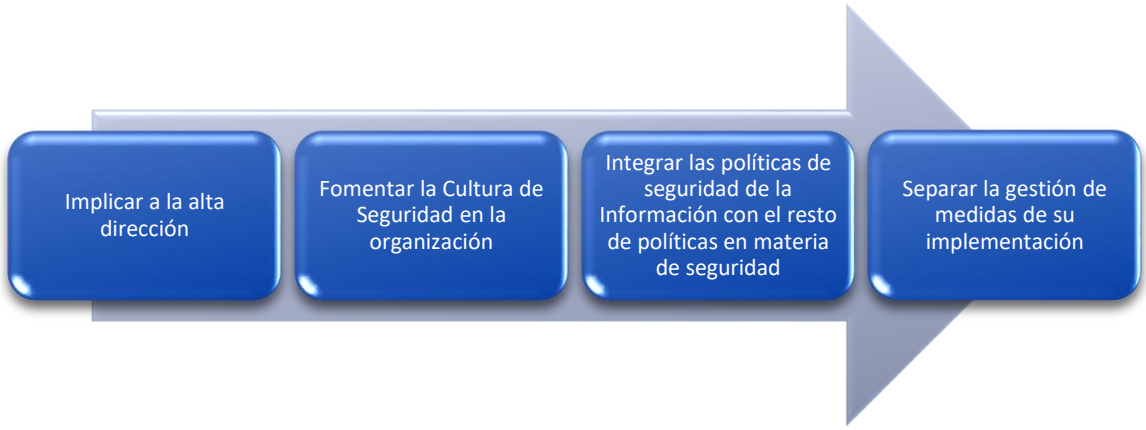


(Meyer, 2014).

La norma ISO 27001 determina que la seguridad de la información es "la preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad y confiabilidad" -. La figura pretende ilustrar aspectos a tener en cuenta para abordas la seguridad de la información y qué ítems se integran dentro de cada una de las seguridades a las que se ha hecho referencia. Si se presta atención a los ítems que engloba cada una de las parcelas de seguridad, se aprecia una clara distinción funcional entre ambas. A bote pronto, cabría pensar que mientras que la seguridad de la información se preocupa de aspectos de gestión, control y análisis, la seguridad informática trata únicamente aspectos tecnológicos, sin prestar atención a las tareas de gobierno. Nada más lejos de la realidad, llegar a tal afirmación sería un craso error: la implantación de medidas tecnológicas requiere no sólo la aplicación de medidas técnicas; además requiere de una estrategia, de una serie de políticas de seguridad –

reglas en firewalls y routers, distribución de antivirus- y de la subsunción de estas medidas con las diferentes recomendaciones ISO, recomendaciones de las agencias nacionales e internacionales de materia de seguridad, etc.

La siguiente duda razonable es bajo que figura debe recaer tal responsabilidad, teniendo en cuenta los siguientes aspectos que recoge la norma ISO y a los que ya se ha hecho referencia:



A lo largo de la investigación, y desde una perspectiva holística, se abordará tal interrogante con el objetivo de determinar si la figura a la que se hace referencia debe estar integrada en el departamento de seguridad corporativa.

6.2.4 Nuevos roles profesionales

Tanto la normativa ISO como la directiva NIS actúan de bisagra para la incorporación de nuevos perfiles profesionales relacionados con la tecnología de la información. Uno de estos perfiles es el conocido como CISO –Chief Information Secutity Officer-. La proliferación de los ataques informáticos, tanto en número como en intensidad, y la importancia que adquiere actualmente la información en el seno de las empresas, han puesto de manifiesto la necesidad de incorporar este perfil lejos de la figura del responsable de sistemas – CIO o Chief Information Officer-. Actualmente esta figura está adquiriendo un papel cada vez más relevante *por mor* de la ya mencionada importancia de la información. Una información bautizada por algunos como el petróleo del SXXI. Es en organizaciones con mayor madurez y evolución donde esta figura se hace presente.

Así pues, la realidad exige un nuevo paradigma que aleja orgánicamente la figura del CIO y la del CISO. La separación funcional ya existe puesto que al CIO le corresponden tareas de

implementación y desarrollo de la tecnología mientras que el CISO tiene como labor principal garantizar la seguridad de la información dentro de la organización y asegurar la implementación de las medidas de control para tal efecto (Koegler, 2015) o, dicho de otra manera, el rol del CIO es operacional mientras que la del CISO se orienta reducir el riesgo. El ámbito funcional de ambas figuras les conduce a mantener una relación un tanto controvertida (ComputerWorld.com, 2011) .

El CISO, no sólo debe tener conocimientos en tecnología, sino que adicionalmente debe estribarse en concienciar a los usuarios de los riegos del uso inadecuado de la tecnología, realizar análisis de riesgos, administrar la seguridad de la información y definir la política de seguridad a seguir (seguridadamericana.com, 2017). Su éxito radicará, en gran medida, en establecer estrategias para combatir ataques alejados de la heurística que caracteriza a la mayoría de ellos.

Tal como apuntaba la normativa ISO, la comunicación es fundamental para poder ofrecer seguridad a un sistema. De aquí se desprende una de las habilidades necesarias que deberá incorporar en su currículum el CISO: deberá traducir a un lenguaje de negocio, las necesidades en materia de seguridad. Se infiere que no sólo debe manejar un lenguaje técnico sino además económico (Catarino, 2016). Esta comunicación deberá ser, además, transversal al elenco de departamento propios de cualquier organización ya que hoy en día no se concibe separar el negocio de las empresas de sus necesidades de seguridad (Capitalhumano.com, 2016).

Asimismo, deberá empatizar con el usuario y saber pensar como él para así poder anticiparse a los problemas. Es importante señalar la importancia de tal afirmación a sabiendas, como se verá en epígrafes sucesivos, que el usuario es una de las principales amenazas de las organizaciones. Tanto si esta figura se encarna en un sola persona o en un departamento, es importante estar al día en cuanto a formación y que el personal que integre esta figura tenga la formación y experiencia adecuada dado que "*es imposible proteger algo si se desconoce cómo hacerlo*"(Silicon, 2014).

6.2.5 El binomio ciberseguridad sociedad

España cuenta con 31 millones de internautas, lo que supone una tasa de penetración del 65,5% de su población. El estudio del ONTSI -observatorio nacional de telecomunicaciones y sistemas de la información- de abril del año 97, realizado por el Ministerio de Industria, analiza cuál es el nivel de confianza en la red y de ciberseguridad por parte de los españoles. Según el estudio, más del el 42,1% confía bastante o mucho en internet y únicamente el 2,2% de la población desconfía de Internet. El 42,5 % de los internautas perciben Internet cada día como más duro.

El 69% de los internautas consideran su equipo informático o dispositivo móvil razonablemente protegido frente a las potenciales amenazas de navegar por la red. Tres de cada cuatro usuarios consideran que no se usa adecuadamente el software que disponen y dos tercios creen que la propagación de las amenazas se debe a la poca cautela de los usuarios. Casi la mitad de los encuestados piensan que es necesario asumir ciertos riesgos para disfrutar de internet.

Los datos revelan que las redes WI-fi se han convertido en un elemento cotidiano para cualquier usuario. No obstante, la mayoría de ellos no son conscientes de los riegos que conlleva conectarse a una red insegura o mal configurada, y se conectan siempre que lo necesitan y en cualquier lugar, sin comprobar el nivel se seguridad que ofrece el router o red WIFI.

El elemento que reviste mayor gravedad es el ordenador personal. A pesar de que la gran mayoría de los encuestados considera su equipo protegido, en el 63,9 % de ellos se ha encontrado malware y en el 71,8% de estos casos era considerado malware de riesgo alto (Ministerio de Industria, 2017).

El desconocimiento en materia de seguridad, la asunción de riegos como algo natural, y el exceso de confianza en el uso de la tecnología, no es algo exclusivo de los internautas españoles. Alumnos de la Universidad de Illinois, Urbana Champaign y la Universidad de Michigan, elaboraron un experimento conjunto denominado “Users really do plug in USB Drivers they find” que consistía en distribuir aleatoriamente en un campus universitario 297 memorias USB infectadas con un malware. Sólo bastaron 6 minutos para infectar la primera máquina, y la tasa de efectividad fue del 45-98% (M. Tischer *et al.*, 2016).

La falta de conocimientos y de cultura de seguridad no pasa desapercibida ante la mirada avizor de los ciberdelincuentes, que están al acecho de los descuidos y de las prácticas inseguras de los

usuarios. Tal problemática debe abordarse formando a los usuarios, dando un giro de 180 ºC de tal manera que se integre al usuario como parte de la respuesta a la amenaza a modo de *human firewall* (Marzo, 2017).

Similar escenario se plantea en el seno de las organizaciones *por mor* que los actores son los mismos que en la platea privada. En este sentido, es interesante traer a colación el informe que Kapersky Lab, -empresa líder en seguridad informática- presentaba el pasado mes de Julio y que se hace eco de la realidad a la que se ha hecho referencia. Según el informe, sólo el 12% de empleados encuestados, es consciente de las políticas y normas de seguridad informática implantadas en su organización. El 24% de los empleados considera que no existe en su empresa ninguna medida de seguridad (elEconomista.es, 2018b).

Tal afirmación va acompasada con el hecho que el factor humano sea el eslabón más débil en la cadena de la seguridad. Otra investigación llevada a cabo por la misma compañía, refleja que el 46% de las empresas españolas admiten que los empleados son su principal vulnerabilidad en materia de seguridad de la información. Tal es así que el 40% de los empleados tiende a esconder debajo de la alfombra los incidentes relativos a la seguridad haciendo, de esta manera, que sus empresas sean mucho más vulnerables. Una cifra preocupante si se tiene en cuenta que el 29,6 % de los ataques dirigidos a las empresas españolas utilizan pishing e ingeniería social como artimaña para acceder a la información de la organización. Los ciberdelincuentes encuentran en el empleado la pasarela perfecta para llevar a cabo sus fechorías (Pankov, 2017).

Nuevamente el concepto de cultura de seguridad adquiere gran importancia y se establece como medida urgente para ofrecer soluciones adecuadas a la miscelánea de amenazas de la red. No debe pasarse por alto que esta cultura de seguridad no sólo se refiere al usuario y su conocimiento de los riesgos intrínsecos del uso de los sistema de información sino también al personal de dirección y de RRHH (KaperskyLabs, 2017). La cultura de seguridad de estas figuras requiere, además de la cultura de usuario que se acaba de referir, de una cultura de seguridad relacionada con su cargo. El hecho que los usuarios escondan debajo de la alfombra los incidentes de seguridad de los que han sido "colaboradores necesarios" obedece en muchas ocasiones a la implantación de políticas de seguridad basadas en la sanción y castigo en lugar de la comunicación y de una cultura de ciberseguridad positiva. No se trata de imponer las medidas de seguridad *a fuer* de sanción sino de incentivar estrategias que se hagan valer de otros

mecanismos alejados de cualquier imperativo. Entre estas estrategias la educación y formación en materia de seguridad se enarbola como una de las mejores opciones para empapar al empleado de la tan necesaria cultura.

7. CASO DE ESTUDIO

La presente investigación aborda la situación de la seguridad corporativa en España de un modo amplio. No se contempla ningún escenario en concreto, ni se pretenden realizar estudios comparativos. La ambición de la presente pasa por establecer unas líneas genéricas de la situación actual de la seguridad corporativa en España y analizar si se corresponden y dan respuestas a la pléyade de riesgos y amenazas que deberían dibujar sus líneas de actuación del presente y del futuro.

Las inferencias que del proceso dimanen deberían ser el punto de partida para desarrollar una teoría que determine *de iure* y *de facto* cómo configurar los departamentos de seguridad corporativa del entramado empresarial español. En definitiva, sembrar las bases de una herramienta al alcance de los empresarios destinada a ofrecerles garantías en aras de salvaguardar sus más valiosos activos, una herramienta enfocada a ofrecer una visión holística e integral de la seguridad.

8. DESARROLLO DE LA INVESTIGACIÓN

A lo largo del siguiente capítulo se pretenderá enhebrar el marco teórico y el análisis documental en la pregunta de investigación planteada con el objetivo de hilvanar una línea argumental que coadyuve a determinar, por un lado, la respuesta a la pregunta de investigación y por el otro contrastar las hipótesis y variables planteadas.

Dicha maniobra requerirá horadar las diferentes entrevistas realizadas como complemento de primer orden al marco teórico y análisis documental tratados en capítulos anteriores.

8.1 Seguridad física y personal: una perspectiva tradicional pero necesaria

La seguridad privada se ha asociado tradicionalmente a la figura del vigilante de seguridad, a las cámaras de vídeo vigilancia, alarmas y alguna que otra medida adicional. Esta percepción

encuentra su razón de ser, en gran parte, en el compendio normativo. Esta concepción encorsetada es similar a la que nos presenta tanto la antigua ley 23/1992 como la nueve LSP y el reglamento que la desarrolla por lo que respecta a las actividades, servicios y medidas de seguridad otorgadas al personal de seguridad privada. A pesar de las tendencias neoliberales y a las dificultades crematísticas de los estados, el legislador parece nadar a contracorriente *por mor* que el abanico de actividades y servicios que la nueva LSP establece dista muy poco del marco normativo anterior a pesar de los 22 años que los separan.

Es precisamente el resumen de actividades y servicios – artículo 5 y 38 de la LSP- el que da buena cuenta de la visión un tanto miope de la seguridad privada. No obstante lo dicho, se debe señalar que se trata de una parte troncal y fundamental de las funciones del personal de seguridad privada. Tanto es así que uno de los denominadores comunes del elenco de entrevistas realizadas a los directores de seguridad es que desde todos los departamentos de seguridad se da respuesta a amenazas que requieren ser contrarrestadas mediante estas actividades, servicios y medidas de seguridad. Básicamente se trata de dar respuesta a amenazas contra el patrimonio de las empresas, la seguridad y protección de sus empleados, clientes y personas que se pudieren encontrar en sus instalaciones e incluso, tal y como se desprende la entrevista realizada al director de seguridad adjunto de la Universidad Autónoma de Barcelona, para dar respuesta a riesgos medioambientales (Sánchez, 2018).

Entidades como el Banco de Sabadell, Caixabank e incluso la Diputación de Barcelona, consideradas grandes corporaciones desde un punto de vista estructural, han configurado sus respectivos departamentos de seguridad con varias subunidades dedicadas a la gestión de este tipo de amenazas que requieren de las actividades mencionadas (Vivancos, 2018), (Zamora, 2018) y (Capell, 2018). A pesar de ello, en el resto de entidades también se observa una estructura análoga a pequeña escala que acostumbra a pasar por la subcontratación de vigilantes de seguridad dedicados a la protección de personas y patrimonio, que pueden estar coordinados en algún caso por algún jefe de equipo y gestionados en última instancia por el director de seguridad. Por lo que respecta a la configuración mencionada, se observa que obedece, por un lado, y en primera instancia, al resultado del análisis de riesgos y por el otro al tamaño del departamento de seguridad, relacionado a su vez con la envergadura de la corporación. Una de las tareas transversales de los directores de seguridad entrevistados es

precisamente, recoger diariamente las incidencias e informes de seguridad que dimanan de estas estructuras o unidades.

Esta versión más tradicional de la seguridad, en adelante seguridad física, es intrínseca en todos los departamentos de seguridad y, por lo tanto, uno de los pilares básicos de la seguridad corporativa.

8.2 La inteligencia en el seno de los departamentos de seguridad

"Yo recuerdo que antes se buscaban carteles y pancartas en las manifestaciones de los estudiantes y era lo que buscaban los Mossos d'Esquadra, a ver quién colgaba esos carteles en las manifestaciones, ... Ahora también miramos las redes"(Sánchez, 2018).

La afirmación del director de seguridad adjunto de la Universidad Autónoma de Barcelona, es sólo un botón de muestra del cambio de paradigma en los departamentos de seguridad de las empresas y el punto de inflexión que explica la metamorfosis de la seguridad física, a la que se refería el epígrafe anterior, a otro concepto de la seguridad basado en la prevención y, en alguna ocasión, en la alineación de la estrategia de seguridad con la estrategia de negocio; una concepción mucho más cercana a la seguridad corporativa.

Todos los directores de seguridad coinciden en que de una manera u otra hacen inteligencia y que ésta se ha convertido en la principal arma para anticiparse al riesgo. La prueba del nueve es que antaño las empresas de seguridad se ceñían a contratar vigilantes y cámaras de seguridad y en la actualidad se demandan y subcontratan servicios de inteligencia. Por otro lado, las grandes corporaciones y las empresas de seguridad están integrando en sus plantillas analistas de inteligencia. "*Los directores de seguridad tenemos que ser conscientes de que el pilar fundamental de la protección pasa por la inteligencia".* (Franco, 2018).

Tal y como afirma el ex director de seguridad del Banco de Sabadell (Zamora, 2018), la inteligencia es uno de los valores intrínsecos de los departamentos de seguridad y ha permitido el cambio de paradigma al cual se ha apuntado al principio del epígrafe. A pesar de que ha sido una práctica que siempre se ha utilizado, ha sido la sociedad de la información quien la ha catapultado hasta ocupar el lugar preferente que ocupa actualmente en el seno de los departamentos de seguridad. La proliferación de las fuentes de información abiertas –OSINT- , de la tecnología, de Internet y de las redes sociales, son alguna de las variables que sirven para

explicar este nuevo paradigma que ha supuesto un cambio de enfoque *per se* en la manera de abordar la seguridad.

Es importante señalar la simbiosis de esta herramienta con otra fundamental –el análisis de riesgos- que la LSP pone a la merced de la figura del director de seguridad en la atribución de sus funciones. La inteligencia y el análisis de riegos van de la mano en aras de ofrecer soluciones de seguridad integral. De nada o más bien poco serviría disponer de un análisis de riesgos si no puedes hacer frente de forma preventiva a las amenazas. Asimismo, carecería de sentido trabajar la inteligencia sin tener acotadas las amenazas.

De la misma manera que ocurre con la seguridad física, el tamaño del departamento condiciona la integración de la inteligencia. Mientras que en las PYMES, la inteligencia la aborda directamente el director de seguridad, subcontratando en ocasiones algunos servicios, como en el caso del departamento de seguridad del Diagonal Mar (Cantero, 2018), en las grandes corporaciones encontramos estructuras formadas por dos o más personas dedicadas a la inteligencia.

Una de las demandas que cada vez adquiere más protagonismo y que a su vez está relacionada con la inteligencia es la protección ante las amenazas o riesgos de carácter reputacional. Cada vez las empresas destinan más recursos para salvaguardar la imagen o la marca de la empresa e incluso de sus empleados. Tal como señalaba durante la entrevista realizada a Selva Orejón, experta en identidad digital y directora ejecutiva de Onbranding, los servicios que más le demandan son: conocer el origen de un ataque con influencia en la reputación o identidad del cliente; la eliminación y transposición del contenido y servicios forenses para determinar las filtraciones de información que hayan podido tener lugar (Orejón, 2018).

Cabe señalar que la concepción del término inteligencia a la que hace referencia en la entrevista el experto en la materia, Carles Ortolà, es un tanto distinta de la que tienen todos los directores de seguridad entrevistados, sin excepción. Para éste, la inteligencia no deja de ser un proceso epistemológico: *"Se trata de una forma de mitigar riesgos conociendo la información, y ¿qué tipo de riegos?, tú te enfrentas a riesgos de carácter reputacional, de carácter estratégico, de carácter económico pero siempre desde un punto de vista holístico*" (Ortolà, 2018). Es precisamente esta visión holística donde radica la diferencia con la concepción de inteligencia, un tanto sectorial – limitada a ámbitos de seguridad- de los directores de seguridad. Tal vez,

como él apunta, el origen de esta concepción naif se deba a la figura tradicional del director de seguridad; al hombre vetusto y desconfiado anclado en la seguridad física y reacio a la nueva realidad y cambio de paradigma que nos blinda la tecnología. " [..] *de repente se encuentran estructuras que había creadas, insisto, medievales y totalmente de reino de taifas , necesitamos adaptarlas a un sistema, a un vocabulario, a unas concepciones o a unos conceptos que son estos de la inteligencia. Las incorporaciones que recientemente se observan en las empresas, obedecen, en muchos de los casos, a una moda que nada tiene que ver con la inteligencia; se trata de analistas de datos científicos, que atienden una parte de las demandas pero no el todo*".

Más allá de realizar un análisis conceptual profuso, interesa señalar que la concepción que profiere Carles Ortolà abraza toda una serie de riesgos que se van imbricando para ensartar una fórmula holística. La estrategia del negocio es una variable fundamental de esta fórmula, de la misma manera que lo es para la seguridad corporativa en la aproximación conceptual realizada en epígrafes anteriores. Bajo esta afirmación, aflora el siguiente peligro: si no se integran factores estratégicos en las soluciones de inteligencia por parte de los departamentos de seguridad, difícilmente podamos estar hablando de seguridad corporativa y difícilmente se puedan ofrecer soluciones de seguridad integral. Si esto es así se corre el riesgo de relegar los departamentos de seguridad a su concepción tradicionalista en la cual dependían estructuralmente de departamentos como mantenimiento, … Esta falta de avidez se ve acrecentada si se tiene en cuenta que la gestión de una de las mayores amenazas del sector privado –el ciberespacio- tampoco se esté llevando en la gran mayoría de los casos, desde el departamento de seguridad. Tal circunstancia será objeto de análisis a renglón seguido y se explica en parte por una falta de conocimiento notable por parte de los directores de seguridad en aspectos tecnológicos que está originando, tal y como señala Carles Ortolà y Selva Orejón, la descentralización en las empresas de servicios de seguridad. Tal aserción pone de manifiesto la necesidad de que el director de seguridad hable un lenguaje mucho más técnico que le permita hacer de correa de transmisión con la dirección de la corporación (Orejón, 2018). Tal necesidad ha sido captada por el mundo anglosajón que ha incorporado en sus masters de seguridad un 60 % de temario destinado a interpretar técnicas de computación, entender algoritmos, … (Ortolà, 2018) .

Cabe señalar además el papel fundamental que juega la inteligencia en cuanto a la relación entre seguridad pública y seguridad privada. Esta casuística será objeto de análisis en un epígrafe posterior dedicado a analizar tal relación.

8.3 Ciberseguridad: una patata caliente

"Los directores de seguridad corporativa nos hemos tenido que reeducar y formar en un ámbito que es la seguridad informática, teniendo en cuenta que la seguridad informática es la seguridad que más atentados y vulnerabilidades tiene. Antes un director de seguridad tenía que mirar los aspectos físicos, que las puertas estuvieran cerradas, que las vayas estuvieran altas, que la gente no perdiera las llaves de las puertas. Ahora es lo mismo pero en el ámbito informático. Antes te atacaban por tierra, mar y aire y tenías que mirar cómo protegerte de estos ámbitos. Actualmente hay otro sistema que es el ataque de tus propios sistemas. En definitiva, tienes que mirar por lo mismo, que la gente no se deje puertas abiertas en los sistemas, que pongamos unos muros que son los cortafuegos, sean lo suficientemente fuertes, tenemos que vigilar que la gente no pierda ni deje las llaves,…. En definitiva es lo mismo pero en otro ámbito, la mentalidad en seguridad es absolutamente válida. El conocimiento es lo que nos falta" (Baró, 2018).

Como se hacía referencia en capítulos anteriores, la ciberseguridad ha venido para quedarse. Se han dedicado diversos epígrafes para dar cuenta de tal realidad: toda una infoxicación para acreditar que los riesgos que entraña el ciberespacio es una de las mayores preocupaciones de las empresas. Existe toda una literatura que refuerza tal aserto y que determina que las empresas están dedicando cada vez más recursos económicos y humanos para paliar las nuevas amenazas inherentes al nuevo ecosistema. El caso español no es ninguna excepción. Los ocho directores de seguridad entrevistados señalan el ciberespacio como una de las principales amenazas para los intereses de sus empresas. Sin embargo, en ninguno de los casos de estudio la ciberseguridad se lleva exclusivamente desde los departamentos de seguridad. En definitiva, todo un torpedo a la línea de flotación de la seguridad integral.

Existen diversas variables explicativas para esta realidad. La primera de ellas es la falta de formación de los directores de seguridad en materia de Ciberseguridad. Solo uno de los directores entrevistados tiene formación en Ciberseguridad. "E*s imposible proteger algo si se desconoce cómo hacerlo*"(Silicon, 2014). Este desconocimiento es extrapolable al conjunto de la sociedad. Tal y como señala Nicolás Castellano, experto en Ciberseguridad, profesor de la

Universidad de Barcelona y General Manager en Andubay *" Hay un lema o un estigma que se está lanzando qué dice que las nuevas generaciones son las que están más preparadas tecnológicamente y de hecho yo estoy viendo cada vez más y de hecho en grados universitarios veo que hay poca gente que realmente esté preparada tecnológicamente, hay más gente que parte de cero".* Tal afirmación trae a colación otra realidad en lo que se refiere a ciberseguridad: El usuario es la principal amenaza en materia de ciberseguridad. Para vencer a la amenaza en forma de usuario la mejor arma es la cultura de seguridad; una cultura de seguridad que debería emanar del director de seguridad que ya hemos visto que no tiene formación en ciberseguridad. En definitiva, un callejón sin salida. "A*ntiguos policías, que los reciclan que no tiene la visión de ciberseguridad y que los meten en este espectro y que luego forzadamente porque no es un tema de vocación que se ven sometidos a entrar en el mundo de ciberseguridad. Ven la informática como un mundo de brujería porque hay aspectos inexplicables para ellos*" (Castellano, 2018)

Otra de las variables que explican el por qué la ciberseguridad no se esté llevando desde los departamentos de seguridad se atribuye a aspectos históricos de la propia corporación (Zamora, 2018). Tal y como señala el ex director de seguridad del Banco de Sabadell, la ciberseguridad o lo que antes se conocía como seguridad informática, se ha gestionado siempre desde los departamentos de sistemas. Actualmente las entidades financieras son las que más ataques cibernéticos padecen (Castellano, 2018) y (Arana, 2017) y sin embargo, tanto en Caixabank como en el Banco de Sabadell, la ciberseguridad se gestiona desde el departamento de sistemas. Únicamente se observan prácticas de *benchmarking* en la que se ponen en común experiencias, ataques, etc. La nula formación en materia de seguridad y la historia de la propia entidad son dos de las variables explicativas de tal circunstancia, a las que cabría añadir el recelo natural por parte de los departamentos de TI a desprenderse de esta función o, peor aún, a ser fiscalizados por el departamento de seguridad.

No ofrece ninguna duda que las auditorías contables realizadas por los propios departamentos de finanzas no tienen el mismo valor que las mismas auditoria encargadas a órganos externos. En cierta manera el hecho que la ciberseguridad esté integrada en el departamento de sistemas conduce a la misma conclusión. De hecho, la normativa ISO, y las corrientes anglosajonas son reacias a esta coyuntura y subrayan la necesidad de separar la implementación de las medidas del análisis de las mismas; separar la ciberseguridad de los departamentos de sistemas.

El siguiente fragmento de la entrevista a J. Luis Franco, director de seguridad de la torre Mapfre de Barcelona sintetiza lo dicho anteriormente y apunta la manera de reconducir dicha situación:

"*Estamos pasando por alto y dejando la ciberseguridad en manos de grandes profesionales de la tecnología, pero no profesionales de la seguridad o defensa por decirlo de alguna manera y ahí tenía que haber unas sinergias ….. hay que ponerse las pilas y trabajar y sobre todo dotarse de conocimientos porque en un mundo de la información, … El departamento de Seguridad tiene que integrar la ciberseguridad y la defensa de la corporación y los datos de la corporación. Entonces el director de Seguridad sí que tiene que cambiar creo que sí a ese perfil qué es una persona que entienda y sepa y le de valor a la inteligencia como medida de protección primera importantísimo, y segundo que sepa entienda y hable el lenguaje de la ciberseguridad*" (Franco, 2018). Esta estrategia es la que ha seguido Joan Miquel Capell, director de seguridad corporativa en la Diputación de Barcelona consiguiendo implicar al departamento de seguridad en materia de ciberseguridad, un ámbito exclusivo hasta su llegada del departamento de sistemas.

El análisis de riesgo de las empresas sitúa el ciberespacio como una amenaza de primer orden; una nueva y deletérea realidad que malmete sus intereses y que sin embargo se está gestionando al margen de la visión global, holística e integral que se le supone al departamento de seguridad. Las variables objeto de investigación "formación del director de seguridad" en concomitancia con la variable "historia del departamento de seguridad" ganan la partida a la variable "amenazas y riesgos".

8.4 Epifanías del hieratismo normativo

Como estrategia de investigación y, dado el exiguo marco teórico, se ha optado por el análisis normativo intentando para establecer una relación de causalidad entre éste y algunas de las realidades manifiestas del sector de la seguridad privada. Las entrevistas realizadas son la prueba del algodón de estas epifanías a las que ya se ha hecho referencia.

La primera de ellas se ha tratado en el epígrafe dedicado a la visión tradicional de la seguridad, o seguridad física y hace referencia a la visión minimalista que ofrece el compendio normativo en los que respecta al elenco de atribuciones al personal de seguridad privada. Esta estenosis funcional contrasta con los análisis de riesgo de todos los directores de seguridad que han sido entrevistados que apuntan a una pléyade de riesgos que requieren de medidas ajenas a las que determina el contenido normativo. Esta dicotomía entre lo que debe ser y lo que es, encuentra

en el director de seguridad una figura catalizadora, un comodín necesario para explicar esta diferencia funcional. La LSP abre un halo de claridad al atribuir en su artículo 36, una serie de funciones de gestión del riesgo de las que se infiere una visión integral y menos carcunda a la que el artículo 5 de la misma ley hace referencia.

Sin embargo, para poder ofrecer soluciones integrales de seguridad, es condición *sine qua non* tener conocimiento en distintas materias y, sin ir más lejos, se ha comprobado que ninguno de los directores de seguridad tiene formación en ciberseguridad, con el agravante que el ciberespacio se ha convertido en la principal amenaza para el tejido empresarial. Vemos que la formación actúa de trombo en la gestión normal de la seguridad.

La visión tradicionalista sirve para explicar, en cierta manera, la capitalización de los puestos de director de seguridad por los ex miembros de las Fuerzas y Cuerpos de seguridad del Estado. La asunción de la seguridad como algo casi exclusivamente físico podría explicar la presencia de ex funcionarios, con un amplio bagaje en la gestión de equipos y de dispositivos de seguridad. Aquellos miembros que habían pertenecido a escalas ejecutivas y superiores, disponen mayoritariamente de carreras universitarias normalmente relacionadas con derecho o criminología que, junto con la agenda de contactos y la experiencia en seguridad han servido de variables para decantar la balanza a su favor frente a un parvo mercado de candidatos idóneos (Franco, 2018). Cabe recordar que el artículo 29 de la LSP condiciona la habilitación de director de seguridad a la obtención de un grado universitario relacionado con la seguridad y que la INT/318/2011 condona tal requisito si se acredita cinco años de experiencia en la gestión de la seguridad y se supera un curso.

"Pero no me han enseñado a hacer un análisis de riesgo ni un plan de seguridad, ni una coherencia sensata del día a día de lo que es Montserrat. ¿Qué tiene que ver un teniente coronel con un departamento de la Seguridad? No tiene que ver nada. aquí entramos en el concepto de Seguridad Pública y de seguridad privada [..] Un director de seguridad debe ser un licenciado, un graduado en seguridad le guste a quién le guste porque yo como director de Seguridad ocupo un cargo directivo. Si usted no quiere seguridad tendrá otra cosa..."(Alcantarilla, 2018).

La gran mayoría de directores de seguridad, reconocen la existencia de una falsa creencia de que la seguridad pública se puede comparar con la seguridad privada y que, por lo tanto, el hecho de ser un ex policía no debería ser, *per se,* un valor añadido para ocupar un puesto de

director de seguridad (Cantero, 2018; Franco, 2018). Adicionalmente los directores que no son ex policías reconocen la facilidad para hacer contactos mientras que los ex policías afirman que la agenda de contactos tiene fecha de caducidad. Por lo tanto, se infiere que la agenda de contactos no debería ser una variable a considerar por las personas encargadas de contratar directores de seguridad. Adicionalmente, cabe señalar, que la dirección de equipos en el mundo policial es jerárquica y se aleja de otro tipo de gestión y liderazgo más propio del sector privado. "*Piensa que tienen una manera de trabajar mucho más jerárquica poco flexible y sometida a la disciplina y no les interesa para su empresa*" (Capell, 2018).

A pesar de ello, las empresas tienen muy en cuenta el *background* policial para la contratación de directores de seguridad y utilizan los cuerpos policiales como cantera para saciar sus necesidades en materia de seguridad integral: "*si tú coges a una persona que haya estado 15 años en el CNI no puedes competir contra esto. Esto no tendría que ser así, pero … pero es así. En mi caso como fue por concurso esto desaparece. Seguramente si no hubiera sido un tema a concurso yo no estaría dónde estoy"* (Sánchez, 2018).

El peso de los riesgos tecnológicos en los análisis de riesgo del sector privado y la presencia de la inteligencia como herramienta inhibidora y preventiva, ha conducido al mundo anglosajón a incorporar en los estudios de seguridad aspectos técnicos acordes a las amenazas vigentes. La mayoría de los entrevistados, señalan que el perfil del director de seguridad del futuro se corresponderá con un perfil mucho más tecnológico y que éste debería ser uno de los valores añadidos que decante su contratación. La siguiente cita, allende el histrionismo que la caracteriza, pretende subrayar la tendencia a la que se ha hecho referencia: "*Cada vez menos planes de autoprotección menos papel menos protocolo muchos de ellos anticuados y mucho más conocimiento generalista técnico especialista*" (Ortolà, 2018).

Se ha dejado entrever en epígrafes anteriores una de las mayores controversias dimanadas del compendio legislativo: la relación entre seguridad pública y seguridad privada. La Constitución Española en su artículo 149.1.29 concluye que la seguridad pública es competencia exclusiva del Estado; sentencias posteriores como la STC 154/2005 y la STC 33/1982 así lo avalan. La llegada de la primera ley de seguridad privada post constitucional -ley 23/1992- ratificaba la relación de subordinación de la seguridad privada respecto a la pública y señalaba que la primera complementaba la segunda. Esta colaboración durante el transcurso de los años, y dadas las

tendencias neoliberales, la crisis de los Estados y la incapacidad para reponer las tasas policiales, ha ido *in crescendo*. La seguridad privada ha ido arañando espacios hasta el momento reservados a la seguridad privada "*se han ido privatizando diferentes ámbitos. Y creo que esta va a ser la tendencia de futuro y creo que la seguridad privada seguirá cogiendo espacio o espacios de la seguridad pública y cada vez más porque veo que los gobiernos se fijan en una idea y es que la seguridad es un gasto y un coste*" (Capell, 2018). La realidad pone de manifiesto que la seguridad privada no sólo ha ganado la batalla en el plano funcional sino en el plano espacial. Esta realidad no ha pasado desapercibida por el legislador quien, en la LSP, ha reformulado los condicionantes de esta relación, una suerte de sofismos si se tiene en cuenta los puntos de vista de los directores de seguridad: "*la diferencia del texto es importantísima antes era de subordinación y ahora es de colaboración, pero resulta que si las que las tienen que aplicar son las mismas mentalidades …. y las mentalidades cuestan mucho cambiar, mucho más que un texto. La mentalidad de los dirigentes policiales, e incluso no hace falta que sean altos mandos sino mandos intermedios, cuesta mucho que cambie, mucho más que el texto de la ley. Al final esta complementariedad sigue siendo bastante subordinada. No quiero que parezca peyorativo, pero sigue siendo: escúchame yo soy la policía, yo soy la administración y tú eres un administrador y tú te tienes que someter a mis peticiones como yo diga*." (Zamora, 2018)

Vemos como mientras la ley habla de complementariedad, la realidad es bien distinta. Nuevamente afloran disfunciones entre lo que debe ser y lo que en realidad es: "*El sector público es muy hermético, muy receloso de su negocio justificado por sus temas sensibles. Esto en Estados Unidos se dieron cuenta que gestionar millones de kilómetros cuadrados es imposible y 22 ojos ven más que cuatro [..] La finalidad de la ley es fiscalizar lo que se está haciendo en el país*" (Ortolà, 2018). A pesar de lo draconiano que pueda parecer, esta idea es, en esencia, compartida por la gran mayoría de los directores de seguridad, tanto ex policías como los que no lo son. El director de seguridad de la torre Mapfre daba cuenta durante la entrevista de la superioridad de los recursos de la parte privada y cómo esto debe ser aprovechado por el sector público. Sin embargo, a renglón seguido y coincidiendo con el director de seguridad de Diagonal Mar, lamentaba la falta de bidireccionalidad de la información. Esta notoria falta de bidireccionalidad de la información es recogida en otros términos por el director de seguridad de Montserrat, ex miembro de las Fuerzas y Cuerpos de Seguridad del Estado: *"usted policía tiene que confiar en mí. Porque usted y yo estamos dentro de la misma familia. Aquí no hay*

personas de primera ni personas de segunda, usted y yo sumamos, yo también soy un profesional de seguridad" (Alcantarilla, 2018);

A pesar de los esfuerzos del legislador para cambiar las reglas del juego, como por ejemplo las comisiones mixtas desarrolladas en la Orden INT/315/2011 – pocas veces llevadas a la práctica, o plataformas de colaboración como RED AZUL, COOPERA o UPIOSP, existe una gran distorsión entre *iure* y facto. La ineficacia de estos organismos para cultivar bases de confianza, se ve contrarrestada cuando el interlocutor de la parte privada es un ex miembro de las Fuerzas y Cuerpos de Seguridad del Estado: "*El hecho de que el director de La Caixa y yo hemos sido policías, esta perdida de confianza queda minimizada bastante porque ellos saben que tú has sido policía […] y de hecho hay veces que les tengo que decir esto no hace falta que me lo expliques porque yo ya lo sé ya he sido policía y noto que esta relación cambia"* (Vivancos, 2018).

Una de las hipótesis planteadas en la presente investigación hace referencia al impacto que tiene la inteligencia en la relación público-privada. Se ha visto, por un lado, como la seguridad privada poco a poco ha ganado terreno tanto en lo funcional como en el plano físico respecto a la seguridad pública. Se trata de una tendencia acrecentada entre otros factores por la falta de recursos de lo público para satisfacer las demandas del mercado. Una realidad que conduce a la seguridad pública de estribarse cada vez más en la retahíla de recursos del sector privado, un hecho que como señalaba Carles Ortolà, ha supuesto un cambio de paradigma de esta relación en Estados Unidos. De igual forma, se ha visto como para la seguridad corporativa la inteligencia se ha convertido en una herramienta de primer orden. Inmersos en una sociedad, la sociedad de la información, donde cantidades ingestas de información circulan por la red, la inteligencia resulta aún más indispensable. Convertir datos en información útil de la que sacar partido y de la que obtener una posición ventajosa se enarbola como prioridad en el seno de las empresas. Unas empresas que sacian esta necesidad a golpe de talonario para incorporar en sus plantillas analistas de datos o subcontratar servicios de inteligencia. Comunidades o agencias de inteligencia con tentáculos en todo el Mundo son auténticos gigantes que permiten fácilmente salvar los obstáculos que la normativa interna de los propios países supone y acceder a la información de una forma eficiente: "*como policía para poder acceder a no sé qué, tengo que rellenar 72 formularios, no sé cuántas firmas y obviamente tengo que tener los recursos y esto alineado con las políticas y las decisiones del gobierno de turno. Finalmente tienes que pelear, … y cuando acabas de pelear te resulta que ya ha pasado el problema. ¿Qué pasa desde un*

punto de vista privado? Pues que es muy muy mucho más ágil Desde un punto de vista estratégico CEO, si tengo un problema llamo a KPMG porque sé que me va a conseguir a esta información por sus tentáculos en todo el mundo. Al final es un tema de eficiencia y es la eficiencia la que funciona en el mundo privado. Aquí para que un policía consiga una información que venga de su compañero de Nantes esto puede suponer la tira de tiempo para conseguir esto, En cambio el de Deloitte llama a su compañero de no sé dónde y le dice dime esto cómo está y en 5 minutos la tienen esta información." (Ortolà, 2018)

La imbricación de estos ingredientes – preponderancia de recursos de lo privado, auge de la inteligencia y sociedad de la información- actúan como comburente de la hipótesis planteada puesto que la información es poder y el sector privado puede permitirse el lujo de pagarlo. Las entrevistas realizadas no sólo revelan esta realidad, sino que también ponen de manifiesto que las empresas reciben información por sus propios medios mucho antes de ser informados por la seguridad pública. "*tenemos un grupo de personas que trabaja diariamente y por lo tanto te enteras de cosas que a lo mejor la seguridad pública tarda más en darse cuenta. En el momento que detectamos alguna cosa que pueda ser de su interés como además estamos obligada por ley se lo facilitamos. Lo que hacemos nosotros muchas veces es obtener información y ratificarla con los cuerpos policiales. A veces te dicen déjame que me lo mire y te digo algo"* (Vivancos, 2018).

8.5 La cultura de seguridad

" Al final la seguridad requiere la corresponsabilidad de todos y la responsabilidad de todos, de los de arriba y de los de abajo y para esto el Director de seguridad debe ser capaz de escuchar y convencer sin imponer su criterio" (Capell, 2018).

El desarrollo de la investigación ha conducido reiteradamente a tratar esta variable a pesar de que no se había previsto *ub initio*. El desarrollo de la misma ha puesto de manifiesto la transversalidad y el protagonismo que adquiere dicha cultura para la implantación de medidas de seguridad integrales.

De la misma manera que la sociedad de la información necesita como antídoto la inteligencia, los riesgos que entraña el ciberespacio en conjunción con la amenaza que supone un usuario neófito e imprudente, necesitan de la cultura de seguridad. Ésta es en sí una herramienta eficiente para combatir las amenazas y al mismo tiempo el cemento perfecto para ligar el resto

de medidas que se implanten en el seno de una corporación. Se trata de la zapata que sustenta los pilares de la seguridad corporativa. Aunque la normativa sectorial no hace referencia alguna a esta función, todos los directores de seguridad entrevistados coinciden en la importancia de la implantación de una buena cultura de seguridad para la consecución de sus objetivos. El director de seguridad es el evangelizador del mensaje, la correa de transmisión entre el departamento de seguridad y el resto de la empresa. Uno de los mensajes que se repiten a lo largo de las entrevistas considerados como el *core* de la cultura de la seguridad consiste en hacer ver al CEO que la seguridad no es un gasto sino una inversión *" La seguridad es un coste necesario no es un gasto, es una inversión, y el 99% de la gente que no tiene cura de la seguridad sabe que la seguridad rebasa la cuenta de explotación. NOOOO!!! totalmente en desacuerdo, lo que hace la seguridad es darle mayor empuje para que todo funcione bien*" (Alcantarilla, 2018).

Como se ha mencionado en epígrafes anteriores, uno de los males endémicos a los que se ha tenido que hacer frente es tener que dotar al departamento de seguridad de entidad propia dentro de la estructura orgánica en el seno de las corporaciones. Un ejemplo más que plausible de cómo llevar a cabo esta labor y que denota con excelencia lo que es cultura de seguridades el caso del ex comisario del cuerpo de Mossos d'Esquadra y actual director de seguridad corporativa de la Diputación de Barcelona, Joan Miquel Capell: "*Yo llego aquí hace 3 años donde el Departamento de Seguridad pertenecía al área de logística, que se dedicaba a elementos o aspectos como la limpieza y también a la seguridad. Cuando yo llego aquí lo separo y actualmente dependemos de Presidencia*". Los mecanismos utilizados para fomentar esta cultura, al margen de las habilidades personales de cada director, pasan por formación, información y concienciación. Todos coinciden que el director de seguridad debe ocupar una posición de poder que le de la autoridad suficiente como para que su mensaje sea tenido en cuenta a todos los niveles de la estructura orgánica de la corporación "*es vital desde el CEO, que entienda que eres una inversión que tú estás invirtiendo en seguridad porque la seguridad si la vamos a buscar la pirámide de Maslow la encontramos enseguida…. que está ahí con lo cual es algo que necesitamos para proyectarnos hacia arriba hacia algo mejor. Esta pedagogía de seguridad pasa desde el CEO hasta el último visitante que entra por la puerta del centro que proteges hasta, el último….*" (Franco, 2018).

No existe ninguna fórmula que determine cómo se debe llevar a cabo tal evangelización. Incluso organizaciones del mismo sector y con estructuras similares optan por estrategias bien distintas.

Es el caso de dos entidades financieras con plantillas superiores a los 20.000 empleados y con delegaciones por todo el estado. En el caso de Caixabank, la estrategia pasa por formar a los empleados, utilizar la intranet corporativa y desplazarse a la delegación cuando ésta haya sufrido un incidente de seguridad. En cambio, en el Banco se Sabadell apuesta por otra estrategia que consiste en hacerse valer de las direcciones corporativas y las direcciones de red territorial para delegar en ellas la función evangelizadora. A través del departamento de RRHH, a cada uno de estos directivos se les atribuye, al margen de sus objetivos a nivel de negocio, la responsabilidad de transmitir esta cultura de seguridad (Zamora, 2018). Sin duda alguna, esta fórmula requiere de una madurez sólida en materia de seguridad adquirida mediante un proceso de años de trabajo en este sentido.

9. CONCLUSIÓN

La seguridad se ha convertido en una de las mayores preocupaciones de nuestra sociedad. Una sociedad bautizada como sociedad del riesgo en la cual la tecnología y la ciencia han amplificado el espectro de lo que hasta su proliferación conocíamos como riesgo. La fragilidad de los escenarios que se plantean, lo que conocemos como seguridad líquida, enarbola el dilema de cómo reaccionar a situaciones futuras, en muchos casos impredecibles, dificultando las medidas de prevención.

Los nuevos riesgos nos conducen a nuevas formas de afrontarlos, así como de prevenirlos. La monitorización y vigilancia de la marca, así como la elaboración de inteligencia para la toma de decisiones ya no tiene exclusividad del sector público. Cualquier gran organización cuenta con estas estrategias para proteger su seguridad física, lógica y sus intangibles.

La seguridad se desarrolla en el seno la sociedad y, por lo tanto, evolucionará bajo sus demandas. Esto explica el cambio de paradigma por lo que respecta a la seguridad en el transcurso de los últimos decenios. Tradicionalmente las funciones del personal de seguridad privada se han asociado a un concepto de seguridad física basado en vigilantes de seguridad y en ciertas medidas de seguridad como alarmas y vídeo cámaras. Tales medidas fueron pergeñadas para atender a una serie de amenazas determinadas. De esta configuración de la seguridad se hizo eco la primera ley postconstitucional en materia de seguridad privada. Una ley, todo hay que decirlo, que ha dejado un gran poso dificultando así la agilidad en materia de

seguridad que la sociedad demanda. Años más tarde, las amenazas a las que esta retahíla de medidas pretendía hacer frente persisten en esencia. No cabe plantearse, por lo tanto, estrategias de protección que no contemplen estas medidas. Es por ello, que uno de los pilares de la seguridad corporativa es precisamente el que constituye la seguridad física-personal, entendida ésta, como el conjunto de medidas ya mencionado.

Recuperando el hilo del principio del epígrafe, la ciencia y la tecnología han transformado la sociedad de forma profusa hasta extremos impensables. El uso de la tecnología acapara cada vez más ámbitos y más sectores de la sociedad y se extiende a gran velocidad como si de una metástasis se tratara. Sin embargo, su grado de penetración en la sociedad no es directamente proporcional al conocimiento de la seguridad ni a los riesgos a los que nos expone. Dicha circunstancia no escapa del ojo avizor del delincuente y encuentra en esta vulnerabilidad el acicate perfecto para perpetrar sus fechorías. Este hecho explica en gran parte que actualmente las preocupaciones del sector privado en materia de seguridad se centren en hacer frente a esta lacra. Una lacra que aumenta en número y en magnitud a marchas forzadas tal y como revelan las investigaciones.

El teatro de operaciones español, en lo que a seguridad corporativa se refiere, es cuanto menos preocupante: la ignorancia de los riesgos asociados al uso de la tecnología se extiende a los departamentos de seguridad y por ende a la figura de los directores de seguridad de tal manera que ven en la ciberseguridad una patata caliente de la que prefieren no hacerse cargo. En la mayoría de casos es el departamento de sistemas, informática o IT quien se hace cargo de la ciberseguridad. Diferentes normas ISO advierten de la separación necesaria entre la implementación de medidas y la gestión de la seguridad. Tal circunstancia trae a colación la creación de la figura del CISO como responsable de la información y con unas funciones distintas de la del responsable de sistemas. El hecho de que sea el departamento de sistemas quien vele por la ciberseguridad es extrapolable a que el departamento de finanzas se encargue de realizar su propia auditoría; en ambos casos se corre el riesgo de esconder las miserias debajo de la alfombra. Al contrario que en el mundo anglosajón, esta concepción de separar las líneas de gestión e implementación, no ha cuajado en el tejido empresarial español. La formación del director de seguridad, la historia de la propia corporación, así como la animadversión a desprenderse de esta parcela por parte de los responsables de sistemas son algunas de las variables explicativas de este fenómeno.

Esta configuración no es compatible ni con la seguridad integral ni con la seguridad corporativa dado que ni trata de forma holística todas las amenazas ni garantiza la alineación de la estrategia de seguridad con la de negocio.

El director de seguridad debe abandonar los tics tecnofóbicos y formarse en materia de ciberseguridad. No se trata de ser un experto en la materia, sino de tener el conocimiento suficiente como para aplicar una estrategia para paliar los riesgos que su análisis determine. Se trata de dar respuestas a las amenazas existentes en un nuevo ecosistema igual que lo está haciendo con las amenazas tradicionales. De la misma manera que no instala una cámara, pero sí que determina el mejor sistema a instalar, no se le exige implementar las medidas, pero sí determinar cuáles implantar; de la misma manera que determina los criterios de acceso a las estancias de su organización, deberá determinar qué reglas habrá que implementar en un Firewall en función del activo que se quiera proteger. En definitiva, el mismo perro pero con distinto collar.

Sin duda alguna, el legislador debe replantearse la formación exigida para la habilitación de director de seguridad y adecuarla a las amenazas con las que debe enfrentarse sin perder de vista la perspectiva panóptica de éste. El conocimiento permite adoptar posturas preventivas y no tanto reactivas. Además, posibilita ofrecer soluciones integrales; en definitiva, escapar de la realidad actual en la que la ciberseguridad es una patata caliente cocinada lejos de los departamentos de seguridad corporativa.

Mientras tanto, el director de seguridad debería encontrar fórmulas capaces de integrar el conocimiento en materia de ciberseguridad en el seno del departamento de seguridad corporativa, con estrategias que pueden pasar por la incorporación de personal experto, la de la figura del CISO o establecer mecanismos para el traspaso competencial desde el área de sistemas al departamento de seguridad corporativa.

Todo lo que no suponga esta integración de la ciberseguridad en el abanico funcional de la seguridad corporativa es nadar a contracorriente y un craso error desde el punto de vista estratégico puesto que la realidad determina que la ciberseguridad es una de las mayores amenazas del elenco empresarial y por lo tanto debe ser, *de* iure, uno de los pilares de la seguridad corporativa.

El tercer pilar de la seguridad corporativa ha sido fraguado nuevamente *por mor* de las dinámicas sociales. El binomio tecnología y globalización acarrea intrínseco otra nueva realidad. Millones de terabytes campan a sus anchas por la red. En una sociedad bautizada como la sociedad de la información, en la que los datos son el petróleo del S XXI, quien tiene la información tiene el poder. La información hay que protegerla – de ahí la importancia de la ciberseguridad- pero también se tiene que tratar. La inteligencia, tal y como la conocíamos, se ha transformado gracias a la proliferación de OSINT. Se ha pasado de vigilar los mensajes escritos en las pancartas de las manifestaciones a monitorizar la red, Internet 2.0, etc. Esta nueva forma de hacer inteligencia ha abierto una ventana de oportunidad para los responsables de la seguridad corporativa en aras a mejorar la prevención de las amenazas fruto de sus análisis de riegos.

Adicionalmente, se ha observado que la inteligencia está blindando una posición de privilegio a la seguridad privada respecto a la seguridad pública. La frugalidad de la seguridad pública se ve contrarrestada por la aplastante superioridad crematística del sector privado que le permite obtener información de primera mano incluso antes que la seguridad pública, gracias a la superioridad de recursos. Esta realidad hace que la seguridad privada suba algún peldaño en el escalafón relacional, con la aquiescencia del legislador. Hablar de igualdad entre ambas es todo un desiderátum inasible a fecha de hoy, pero en ciernes de ser satisfecho *sine die*.

Esta circunstancia se ve acrecentada por la presencia de lo privado en planos físicos y funcionales reservados antaño a la seguridad pública. Los lindes establecidos por el hieratismo normativo se están desdibujando. Los esfuerzos del legislador para acertar con la fórmula explicativa de la relación público privada no han acabado de dar sus frutos. La complementariedad *de iure* es una subordinación *de facto* relegando a la categoría de sofismos todos los esfuerzos que hace en la exposición de motivos la nueva LSP subrayando cuestiones como colaboración y coordinación. En definitiva “ver, oír e informar”. La falta de confianza del sector público en el sector privado es un denominador común en el conjunto de entrevistas objeto de la investigación. La confianza pasa por la *bona vides* del funcionario de turno y no por fórmulas legislativas. Por lo tanto, el legislador debe captar esta realidad y proponer fórmulas factibles para inhibir tal deletérea realidad y acrisolar dicha relación. La seguridad no es un juego tronos, ni tampoco un juego de suma cero. En este sentido, la confianza debe ser una de las variables en la ecuación relación público privada, si se tiene en cuenta que la seguridad no es cosa ni de unos ni de otros, es cosa de todos.

Huelga decir que una vez establecidos los pilares de la seguridad corporativa – seguridad física-personal, inteligencia y ciberseguridad-, es menester hacer referencia a la cultura de seguridad. Ésta se posiciona como cemento necesario para hacer ligar cualquier medida de seguridad que emane de la dirección corporativa. A pesar de que la ley no hace referencia, se trata de una de las funciones más importantes del director de seguridad, en especial en un escenario donde en materia de ciberseguridad el usuario es la principal amenaza y el elemento más vulnerable en el seno de las organizaciones.

No se ha pretendido investigar si aspectos como el safety, protección de datos e incluso riesgos laborales deben formar parte de lo que se conoce como seguridad integral – todo un oxímoron si se tiene en cuenta el carácter poliédrico de la seguridad-. No obstante, cabe señalar que su fórmula variará dependiendo del análisis de riesgos de la actividad, pero como condición *sine qua non* deberá incorporar la cultura de seguridad como una de sus variables.

El carácter polimórfico de la seguridad debe ser tenido en cuenta como uno de los principales riegos con los que lidiar. La manera de hacer frente a esta realidad es configurar estructuras flexibles en el seno de los departamentos de seguridad corporativa que permita adaptarse a la sociedad con la misma velocidad con la que ésta avanza.

Las amenazas a las que el pasado nos tenía acostumbrados explican en cierta manera la suerte de diáspora en forma de ex policías capitalizando los puestos de directores de seguridad. La exigencia de la seguridad corporativa y el calibre de las nuevas amenazas precisan de unos procesos de selección rigurosos basados más en la meritocracia y no tanto en la agenda de contactos. Tales amenazas deben ser cauterizadas desde el conocimiento que profiere la formación en materia de seguridad. Una formación preconizada por el corolario de amenazas inherentes a la tecnología que auguran un perfil de director de seguridad cada vez más técnico, que sea capaz de traducir un lenguaje tecnológico a un lenguaje económico, que sea capaz de alinear la estrategia de negocio con la estrategia de seguridad, que actué de bisagra entre las distintas dimensiones de amenazas y de correa de transmisión entre el departamento de seguridad y el resto de la corporación para poder infundir uno de los activos más importantes en materia de seguridad: la cultura de seguridad.

10. BIBLIOGRAFIA

Alcantarilla, J. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Arana, M. (2017) '¿Cuánto cuesta un ciberataque a las empresas? | Open Data Security', *ODS | Seguridad Informática*, 24 October. Available at: https://opendatasecurity.io/es/cuanto-cuesta-un-ciberataque-a-las-empresas/ (Accessed: 19 May 2018).

Arias, M. (2017) 'Perspectivas de la pequeña empresa en España', p. 24.

Balan, S. *et al.* (2017) 'Data Analysis of Cybercrimes in Businesses', *Information Technology and Management Science*, 20(1). doi: 10.1515/itms-2017-0011.

Barbero, H. R. (2001) 'La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía', 1, pp. 1816–1827.

Baró, B. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Bosch, J. L. *et al.* (2004) 'Estado, mercado y seguridad ciudadana. Ánalisis de la articulación entre la seguridad pública y privada eb España', *Revista Internacional de Sociología*, 62(39), pp. 107–137.

Briggs, R., Edwards, C. and Pickard, J. (2006) *The business of resilience: corporate security for the 21st century*. London, England: Demos.

Cantero, J. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Capell, J. M. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Capitalhumano.com (2016) 'CISO: El nuevo responsable de la seguridad de la información en las organizaciones', *Capital Humano*, 9 June. Available at: http://capitalhumano.emol.com/1325/ciso-responsable-seguridad/ (Accessed: 21 May 2018).

Castellano, J. N. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Catarino, T. M. (2016) 'The Role of the Chief Information Security Officer', p. 50.

Claret, X. (2015) 'Concepto de Sociedad de la Información'. Available at: http://funredes.org/socinfodo/pres/DP1.pdf.

ComputerWorld.com (2011) *CIO vs CSO: una relación controvertida*, *CSO España*. Available at: http://cso.computerworld.es/actualidad/cio-vs-cso-una-relacion-controvertida (Accessed: 21 May 2018).

Conversia (2018) 'El coste económico de los ciberataques en 2017| Conversia', *Servicios de la Sociedad de la Información, e-commerce e Internet*, 21 February. Available at: http://www.consultoria-conversia.es/internet/coste-ciberataques-2017/ (Accessed: 20 May 2018).

D'Antonio, G. (2018) 'Mesa redonda: "Retos de la Seguridadd Corporativa"', in. *VII Congresos directores de seguridad*, Madrid.

DIRECTIVA (UE) 2016/ 1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión de 6 de julio de 2016'. Diario Oficial de la Unión Europea, núm L 194/1.

Dreyer, P. *et al.* (2018) *Estimating the Global Cost of Cyber Risk: Methodology and Examples*. RAND Corporation. doi: 10.7249/RR2299.

Dutta, A. and McCrohan, K. (2002) 'Management's role in information security in a cyber economy', *California Management Review*, 45(1), pp. 67–87.

elEconomista.es (2018a) *España registra en dos meses más incidentes de ciberseguridad que en todo 2014 - elEconomista.es*. Available at: http://www.eleconomista.es/tecnologia-internet/noticias/9040022/03/18/Espana-registra-en-dos-meses-mas-incidentes-de-ciberseguridad-que-en-el-2014.html (Accessed: 20 May 2018).

elEconomista.es (2018b) *La falta de conocimiento en seguridad informática pone en riesgo a las Pymes - elEconomista.es*. Available at: http://www.eleconomistaamerica.cl/telecomunicacion-tecnologia-cl/noticias/8871956/01/18/La-falta-de-conocimiento-en-seguridad-informatica-pone-en-riesgo-a-las-Pymes.html (Accessed: 21 May 2018).

Escuela Superior de las Fuerzas Armadas *et al.* (2016) *Inteligencia: un enfoque integral*. Madrid: Ministerio de Defensa, Secretaría General Técnica.

España. Ley 23/1992, de 30 de julio, de Seguridad Privada.' Boletín oficial del Estado, núm. 186, de 4 de agosto de 1992, páginas 27116 a 27122. https://www.boe.es/boe/dias/1992/08/04/pdfs/A27116-27122.pdf

España. Ley 5/2014, de 4 de abril, de Seguridad Privada'. Boletín oficial del Estado, núm. 83, de 05/04/2014, pp. 28975 a 29024. https://www.boe.es/boe/dias/2014/04/05/pdfs/BOE-A-2014-3649.pdf

España. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada. Boletín Oficial del Estado núm. 8, de 10 de enero de 1995, páginas 779 a 815. https://www.boe.es/boe/dias/1995/01/10/pdfs/A00779-00815.pdf

Fernández, A. V. and Rodríguez, J. M. C. (2017) 'Análisis de las ciberamenazas', *Cuadernos de estrategia*, (185), pp. 97–138.

Fojoz, E. *et al.* (2012) 'La Ciberseguridad Nacional, un compromiso de todos.'

Fournier, A. *et al.* (2015) 'INTELIGENCIA ESTRATÉGICA Y EMPRESAS: Conocer, comprender, actuar, influir'.

Framis, A. G.-S. (2014) 'La madurez del sector de seguridad privada en España: Análisis de su evolución legislativa', *Revista Policía y Seguridad Pública*, 4(1), pp. 53–77.

Franco, J. L. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Gairín, J. (2011) 'LA SEGURIDAD INTEGRAL:Fortalezas, debilidades y propuestas de mejora en los centros de enseñanza obligatoria de España', p. 25.

Garriga Guitart, D. (2015) *Yihad: ¿qué es?*

'Global Risk Report 2018' (2018).

González, C. P. (2014) 'Seguridad Humana', *EUNOMÍA. Revista en Cultura de la Legalidad*, pp. 167–173.

Instituto Español de Estudios Estratégicos (2016) *Ciberseguridad: la cooperación público-privada*. Madrid: Ministerio de Defensa, Secretaría General Técnica.

ISO 27000:2 (2017) *ANSI/ASIS CSO.1-2013 Chief Security Officer (CSO) Organizational Model*. Available at: https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FASIS+CSO.1-2013 (Accessed: 13 May 2018).

ISO27001 (2005) 'Sistema de Gestión de la Seguridad de la Información'.

Izquierdo Carrasco, M. and Parejo Alfonso, L. (2004a) *La seguridad privada: régimen jurídico-administrativo*. 1a. ed. Valladolid: Editorial Lex Nova (Colección Derecho público, no 24).

Izquierdo Carrasco, M. and Parejo Alfonso, L. (2004b) *La seguridad privada: régimen jurídico-administrativo*. 1a. ed. Valladolid: Editorial Lex Nova (Colección Derecho público, no 24).

KaperskyLabs (2017) *El 46% de las empresas españolas admiten que sus empleados son su principal debilidad en la seguridad TI | Kaspersky Lab ES*. Available at: https://www.kaspersky.es/about/press-releases/2017_46-of-spanish-companies-admit-that-their-employees-are-their-main-weakness-in-it-security (Accessed: 21 May 2018).

Koegler, S. (2015) *Where's the dividing line between CIO and CSO?* Available at: https://enterprisersproject.com/article/2015/3/wheres-dividing-line-between-cio-and-cso (Accessed: 21 May 2018).

Linares López, J. and Ortiz Chaparro, F. (1995) *Autopistas inteligentes*. Madrid: Fundesco.

Ljupcho, S. (ed.) (2016) *Meǵunarodna naučna konferencija 'Bezbednosta kako predmet na istražuvanje--pristapi, koncepti i politiki',*.

M. Tischer *et al.* (2016) 'Users Really Do Plug in USB Drives They Find', in *2016 IEEE Symposium on Security and Privacy (SP)*. *2016 IEEE Symposium on Security and Privacy (SP)*, pp. 306–319. doi: 10.1109/SP.2016.26.

Marzo, A. (2017) 'Cuadernos de Seguridad: Seguridad Privada y ciberseguridad: un valor esencial', April, pp. 72–84.

Mediana, E. (2017) *Los ciberataques costaron a las empresas españolas 1,17 millones de euros en 2016*, *MuySeguridad*. Available at: https://www.muyseguridad.net/2017/12/04/ciberataques-empresas-espanolas-1-17-millones-euros-2016/ (Accessed: 20 May 2018).

Meyer, I. C. O. (2014) 'NORMAS ISO DE SEGURIDAD DE LA INFORMACION', p. 13.

Ministerio de Industria (2017) 'Ciberseguridad y confianza en los hogares españoles'.

Ministerio del Interior (2014) *Requisitos específicos*, *Servicios al Ciudadano*. Available at: http://www.interior.gob.es/web/servicios-al-ciudadano/personal-de-seguridad-privada/directores-de-seguridad/requisitos-especificos (Accessed: 12 May 2018).

Orejón, S. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Ortolà, C. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Palomar Olmeda, A. and Álvarez Moreno, A. (eds) (2014) *Comentario a la Ley de seguridad privada*. Primera edición. Cizur Menor (Navarra): Aranzadi (Colección Grandes tratados Aranzadi, 745).

Pankov, N. (2017) *¿Cómo enseñar a los empleados para que no cometan errores?* Available at: https://www.kaspersky.es/blog/human-factor-weakest-link/13666/ (Accessed: 21 May 2018).

Rathmell, A. (2002) 'Towards postmodern intelligence', *Intelligence and National Security*, 17(3), pp. 87–104. doi: 10.1080/02684520412331306560.

Sánchez, F. X. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Sánchez, M. (2007) *La seguridad Corporativa nuevos retos, nuevas exigencias*. 1st edn. Madrid: E.T. Estudios Técnicos.

Seguridad Nacional (2017) 'Estrategia Seguriad Nacional_2017'. Available at: http://www.dsn.gob.es/sites/dsn/files/Estrategia_Seguriad_Nacional_2017.pdf.

seguridadamericana.com (2017) *La función del CISO dentro de las organizaciones | Revista Seguridad en America*. Available at: http://www.seguridadenamerica.com.mx/seguridad-en-la-informacion/noticia-5649-la-funcion-del-ciso-dentro-de-las-organizaciones (Accessed: 21 May 2018).

Silicon, R. (2014) *CISO o la importancia del jefe de seguridad de la información*, *Silicon*. Available at: https://www.silicon.es/ciso-o-la-importancia-del-jefe-de-seguridad-de-la-informacion-56237 (Accessed: 21 May 2018).

Swartz, J. (2005) '2005 worst year for breaches of computer security', *USA Today*, p. B1.

Taplin, W. L. (1989) 'Six general principles of intelligence', *International Journal of Intelligence and CounterIntelligence*, 3(4), pp. 475–491. doi: 10.1080/08850608908435116.

Troy, T. F. (1991) 'The "correct" definition of intelligence', *International Journal of Intelligence and CounterIntelligence*, 5(4), pp. 433–454. doi: 10.1080/08850609108435193.

Vásquez, D. C. (2016) 'Mejoroar la seguridad en la utilización de medicamentos'. Available at: https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/CA/seguridad-en-la-utilizacion-de-medicamentos.pdf.

Vivancos, S. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

World Economic Forum (2017) 'World Economic Forum: Global Risk Report2017'. Available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf.

Zamora, E. (2018) 'Entrevista Personal Como Soporte a la investigación del TFG'.

Zigorraga, I. A. (2006) 'Las competencias estatales y autonómicas en materia de seguridad pública y privada.?` Se opera algún cambio con el nuevo Estatuto para Cataluña?', *Revista Catalana de Seguretat Pública*, (17), p. p–63.

11. ANEXO I, Entrevistas

No se autoriza la divulgación del contenido de las entrevistas del presente epígrafe.

11.1 Entrevista Selva Orejón

FICHA TÉCNICA	
Descripción	Entrevista a Selva Orejon, experta en Inteligencia, OSINT e identidad digital. Directora ejecutiva OnBranding.
Técnica instrumental	Entrevista semiestructurada
Objetivo	Principales demandas por parte de las empresas. Cuál es su relación con los departamentos de seguridad. Nivel de conocimiento percibido en su materia. Gestión de seguridad por parte de las empresas en lo que respecta a la identidad
Fecha	12 de febrero del 2018
Lugar	Instalaciones OnBranding
Observaciones	

1.- Identidad digital, ciberseguridad, inteligencia, reputación Online. ¿Cuál es tu especialidad, ¿cómo se relacionan los otros fenómenos?

Para contextualizarlo, que va a ser lo más sencillo, yo estudié ciencias de la comunicación y me especialicé en gestión de crisis. Empecé a trabajar para diferentes multinacionales, como por ejemplo el grupo ADORFINA??, después en el grupo Gallina Blanca, Anuntis Segunda Mano, y conforme iban pasando los años yo me iba dando cuenta que estando en el departamento de comunicación, concretamente en el área de Internet, que es donde más me metía había muchas de las incidencias que venían por una falta de privacidad: se filtraba información o, por ejemplo, accedían a la base de datos y publicaban parte de ella y como para mí esto era un problema y no había nadie dentro de diferentes organizaciones e instituciones en las que yo estuve que lo gestionase, normalmente la que se acababa encargando era yo porque como esta es la de crisis pues venga, … Estando en España me di cuenta que esto podía ocurrir y por circunstancias de la

vida me fui a vivir a Berlín durante dos años y allí fue donde yo vi la crisis más grande que yo me había encontrado en ese momento a nivel reputacional, en el que habían accedido a nuestra base de datos, lo habían grabado en directo, en youtube Streaming y estaban emitiendo en directo toda la base de datos y estaban pidiendo dinero a cambio de la base de datos, con lo cual todos los medios de comunicación, como era una Startup muy conocida, sobre todo porque nos acababa de comprar en ese momento el grupo Holsfrink, un editorial muy grande de Alemania, nos encontramos con la situación de que esa empresa no tenía la capacidad a nivel de seguridad para poder hacer frente reactivamente al ataque, y ya no te digo nada preventivamente . Era una realidad, no se podía. Entonces ahí empecé a darme cuenta de la importancia primero de poder tener unas buenas políticas de seguridad para que este tipo de atentados que luego iban afectando a la reputación, se pudieran minimizar.

Cuando me fui a vivir a Madrid, esto fue en el 2007 creo, empecé a trabajar para una empresa, que es el grupo planeta y ahí ya sí que, no es que tuviéramos problemas reputacionales, pero sí que es verdad que cogieron nuestra base de datos y la hicieron pública clonando toda la información que había en LANETRO.COM que era uno de los portales que llevábamos. Entonces ahí ya dije esto ya sí que es una realidad. 2007, empiezan las redes sociales y vamos a ir necesitándolo. Y ahí es cuando empecé a hacer las primeras vigilancias digitales. Empezaos con alertas de Google, empezamos con otro tipo de herramientas de monitorización y ya se integró toda la parte de inteligencia, de poder analizar no sólo los posibles tipos de amenazas, pero también cómo lo podríamos utilizar en positivo, empezar a encontrar personas que son líderes de opinión de diferentes públicos, encontrar también otras empresas que lo estaban haciendo de forma diferente y que nos podría beneficiar y entonces ahí es donde ha ido convergiendo todo.

Antes de pasar a la siguiente pregunta, me gustaría que aclararas una cosa que has comentado. Cuando dices que nacieron las primeras preguntas, ¿quieres decir que nacieron de ti?

Bueno, nacieron de mí en el sentido de que el grado de actuación que yo podía tener en las empresas en las que estaba era …. o bien hablaba con el responsable legal o hablaba con el responsable de seguridad corporativa, que seguramente lo que más podía llegar a saber hacer era tener bien configurado e correo electrónico y tener bien configuradas las redes sociales pero

no había como tal una política de ciberseguridad porque no se habían encontrado con la necesidad de hacer nada, claro, en el 2007 …

De acuerdo, luego volveremos a esto con otro tema. La siguiente pregunta tiene que ver con lo que está pasando en la sociedad, en la que cada vez hay más adicción a las nuevas tecnologías, sin embargo, el nivel de conocimiento en la sociedad sobre lo que hay detrás de esta tecnología y os riesgo que entraña, no van acompasados. No es un hecho nuevo, es un hecho que se repite. ¿Cúal es tu valoración al respecto y que crees que habría que hacer para mejorar esta cultura.

Pues tengo muy claro que como el problema principal que tenemos es que hay muchas veces que lo enfocan a los niños, esto no es verdad, los niños no son los que más incidentes tienen, los niños son esponjas y son loros, repiten lo que ven en su día a día y tenemos el gran problema de que tenemos muchas necesidades de relación en las que algunas de ellas han ido mutando, necesitamos relaciones que sean más instantáneas, y esto está ocurriendo no sólo en el ámbito personal sino que evidentemente no está tan diferenciada del ámbito corporativo. Entonces, lo que yo me encuentro es que hay sobre todo una gran carencia de conocimiento emocional, es decir, cómo nos tenemos que relacionar, qué diferencia hay entre la esfera pública y la esfera privada y la íntima, que son diferentes pero que son entendidas como si fueran las mismas; veo también que en relación a los niños, se les está dando muchas herramientas tecnológicas pero no se les está enseñando como poder gestionarlos. Entonces están como auténticos huérfanos…… **Como pollos sin cabeza, ¿no?** Sí

3.- La siguiente pregunta tiene que ver con las tecnologías, no me interesa tanto el pasado, me interesa el presente, pero sobre todo el futuro, ¿cuáles son los riesgos en los que nos tenemos que centrar a medio y largo plazo?

Yo creo que el uso de las tecnologías va a ir cambiando un poco en tanto que hay cada vez más personas que se están dando cuenta que su privacidad tiene un precio no sólo económico sino también desde el punto de vista familiar personal etcétera y que sobre todo en relación al uso de las redes sociales yo creo que va a haber como un tipo de uso mucho más selectivo mucho más activo, es decir, no sólo las escuelas están prohibiendo el que entren los teléfonos (que la verdad que es una pena que esté siendo así) sino que yo cada vez más tengo compañeros de trabajo y también amigos que también están restringiendo el uso de las redes o incluso que también las están cancelando. Entonces yo creo que como normalmente ocurre podemos

coger una tecnología con muchas ganas o una afición o un comportamiento con mucho entusiasmo pero conforme va pasando el tiempo y vamos viendo cuáles son las consecuencias eso se va a ir yo creo que redistribuyendo de una forma natural, es decir, yo creo que no va a haber una explosión del uso de las redes sociales porque ya la ha habido pero sí que se va a ir, se van a ir haciendo de forma quiero pensar que de forma coherente por parte de las plataformas sociales mayores restricciones para poder gestionar contenido; y por parte de las personas también se van a ir limitando en la información, pero los ataques no van a cesar y de hecho yo creo que van a ser cada vez mucho más sofisticados i van a incluir mucho más la ingeniería social sin lugar a dudas porque las medidas técnicas ya se pueden poner.

Ya que hablamos de futuro y, a grandes rasgos, tampoco quiero que me hagas una master clas, pero como he visto que en breve vas a hacer algo relacionado a la nueva ley de protección de datos que todavía no se ha traspuesto pero que lo tiene que hacer ya cómo afectará esto a de la seguridad de las empresas

Yo creo que si dividiésemos las empresas entre pymes y luego grandes empresas, las pymes son las que sin lugar a dudas más afectadas van a estar porque la mayor parte de ellas ni siquiera se han enterado que esto va a ser así, con lo cual no tienen en su presupuesto una partida dedicada para esto ni considero que la vayan a tener por lo tanto vamos a empezar a ver un montón de multas y si pudiéramos hacer un símil con el tráfico la gente se va a ir enterando más por los medios de comunicación que por ellas mismas. En empresas grandes el cambio es evidente ya hay muchísimas empresas que han sido consultadas que ya sí tienen esa partida en sus presupuestos para este año y los próximos años a nivel de implementación.

¿Qué es lo que más te demandan las empresas para que te llaman básicamente y después cuál es tu interlocutor por antonomasia es decir si te llama quién te llama agencia el departamento de sistemas Departamento de Seguridad, ¿cuál es la dinámica?

Pues mira estamos dividiendo los servicios que nos demandan en tres tipos. El primero que nos piden y yo creo que es el más utilizado desde años hasta ahora es el de ciber investigación, es decir, conocer cuál es el origen de un ataque relacionado, en la mayor parte de los casos, con una influencia en su reputación o en su identidad digital. Nos lo están pidiendo empresas que son grandes, pero también nos lo están pidiendo muchas personas que tienen su propia marca personal, por ejemplo, que son celebridades que generan y facturan igual que una multinacional. Luego también nos están pidiendo mucho en relación al primer servicio

eliminación de contenido y transposición de contenido, es decir, encuentran información de carácter privada que se está haciendo pública en Internet y nuestro trabajo consiste en conocer cuál es el origen de la información, pedir la eliminación y en el caso de que legalmente no se pueda, generar mayor volumen de contenidos para que no sea fácilmente encontrable. El tercer tipo de servicio que más nos pueden ir pidiendo, pero por hacemos casi como parte de la investigación son los servicios de forense por ejemplo se ha habido alguna filtración quiere más a conocer cuál ha sido el origen.

¿cuál es tu interlocutor seguramente serán varios, pero es más el departamento de Sistemas el Departamento de Seguridad?

Solamente me contrata o el Director General, presidencia y alguna vez es el abogado de ellos que está buscando que le hagan un peritaje de pérdida de identidad digital o alguna vez algunas veces sí que es verdad que nos llaman desde el Departamento de Seguridad Corporativa porque hay muchos policías y al dar clases en la Escuela de Policía hay muchos de ellos que tienen nuestros contactos y nos llaman.

Pregunta es quién crees que tiene que ser tu interlocutor natural un poquito la línea de lo que decías tú, un departamento de seguridad corporativa.

Bueno cuidado yo creo que no puede ser que haya un único interlocutor de hecho lo ideal sería que nos estuviese llamando desde el gabinete de crisis. Dicho gabinete debería tener un responsable legal o un interlocutor legal un interlocutor de comunicación un interlocutor de seguridad y Dirección General.

Bueno yo tengo mi opinión ¿no?, pero me gustaría saber la tuya y las he y la siguiente pregunta es que si es extrapolable la ignorancia que existe temas de ciberseguridad e inteligencia en la sociedad a lo que vienen siendo los departamentos de seguridad es decir si encuentras carencias graves…

Yo encuentro carencias a nivel de interlocución, dentro de las grandes empresas no hay nadie que esté haciendo de correa de transmisión del conocimiento para poder conseguir que los diferentes departamentos entiendan que la problemática es holística no es una problemática del de seguridad, pero igual resulta que el que está cometiendo una imprudencia digital es uno que está en el departamento de producción y de estos siempre se olvidan en las formaciones.

La siguiente pregunta me la acabas de contestar y si crees que existe una cultura de seguridad en las empresas y que encuentras a faltar

Me encanta que me lo estés diciendo porque yo sinceramente creo que no es algo que solo pase las empresas, sino que en la ciudad en general hay una falta de conocimiento de seguridad brutal. De hecho, es más, y esto es lanzar el capote para todos los cuerpos de seguridad que respeto muchísimo. Tenemos un gravísimo problema con cuáles son los problemas, en que no se está percibiendo cuáles son los trabajos reales que están haciendo los cuerpos policiales. Hay mucha gente que lo único que pueden ver es un señor con una porra o un grupo de personas haciendo una carga policial.

Interrupción llamada XXXX

Hay un desconocimiento brutal es decir no hay cultura de seguridad, es más, no se están percibiendo positivamente los cuerpos policiales porque lo único que se está transmitiendo es, o bien cargas policiales o intervenciones operativas que no son demasiado buenas. Considero que habría que hacer un trabajo muy importante en educar a la ciudadanía.

En lo que coincido también contigo es que la gente no sabe, por ejemplo, el esfuerzo y todo lo que conlleva una investigación y sólo ven el resultado final, aunque todavía si debo decir también que creo que también hay una falta de cultura incluso los cuerpos policiales porque de alguna manera no dejamos, no dejan de ser un reflejo de la sociedad donde creo que falta un poco de cultura y pedagogía.

Bien selva en la línea de lo que estamos hablando ¿tú crees que estés conocimiento en materia de seguridad que encontramos en la sociedad es lo que justifica que la ciberseguridad se esté llevando desde el departamento de sistemas y no de seguridad? A mí no me parece normal.

Totalmente de acuerdo.

¿Cuál es tu opinión al respecto a qué crees que se debe esto?

¿Crees que es un tema de política de empresa de desconocimiento o simplemente es porque del departamento de sistemas no se quieren deshacer del poder?

Esto se debe, yo creo que existe un enorme desconocimiento. Un desconocimiento brutal en quién toma las decisiones. Es igual que en compras. Cómo puede ser que haya situaciones que yo esté viendo en las día a día reacciones en las que se están comprando cantidad ingentes de productos determinados para el uso de la empresa y otros que son imprescindibles como una

VPN por ejemplo para cualquier dispositivo móvil ni siquiera se esté planteando. Es una cuestión de que todavía precisamente por el desconocimiento interno hay muchos directores generales dentro de los consejos de dirección, en los que no hay directores de seguridad o algunos ni siquiera entienden en el conocimiento Seguridad de hecho a los hechos me remito: esta semana tuvimos que ir a dar una clase a una serie de directivos que estaban en el Comité Ejecutivo de una gran empresa y el director de seguridad cuando vio que íbamos con el filtro de privacidad dijo que paranoicos y pensé: perdona con las noticias que acaban de salir abre referencia Puigdemont les pregunté cuántos de vosotros vais en el AVE cada semana cuántos viajáis i vais sin el sin el filtro de privacidad… pues poco ha pasado para lo que os ha pasado porque con la cantidad de boicots que están recibiendo las empresas aquí, que esto todavía se siga viendo como algo que le va a pasar a otro creo que no creo que es un problema de cultura general

Totalmente de acuerdo, incluso en el ámbito judicial cuando les entra un caso tecnología Muchas veces te exigen que llegues me acuerdo por el desconocimiento y el mío a veces que tiene que juzgar algo que tenga que ver con la tecnología.

¿Cuál es tu valoración del perfil, ¿cuál crees que debe ser el perfil del director de Seguridad con qué perfiles te encuentras qué te gustaría encontrarte?

xxxxxinterrupción entrevista de radioxxxxx

Nos encontramos como dos tipos de directores de seguridad: el que viene originalmente de cuerpos policiales y que puede venir de algunas unidades de investigación Criminal u otros que vienen de unidades de análisis de inteligencia que vienen de unidades de información y que están muy acostumbrados a trabajar con información en Internet porque los últimos años es donde más hay. Luego nos encontramos con aquellos que vienen de Unidades de Intervención operativa y que también han entrado a trabajar como director de seguridad o directores de seguridad que se han tenido que ir reciclando que no vienen de ningún cuerpo de seguridad y que vienen del mundo de la seguridad privada y que se tienen que formar a través de proveedores externos de un conocimiento que no tienen o hay veces que sí que tienen conocimiento pero no tienen le falta las manos porque no tienen recursos dentro de su empresa

Lo que observo, con los conocimientos en seguridad adquiridos durante el grado y los que adquirí la Academia de Policía me planteo el por qué los puestos de dirección de seguridad se están cubriendo en muchos casos con policías. Lo hago desde una perspectiva crítica porque para mí la seguridad es algo más volviendo un poquito a lo de antes, es decir la seguridad

siempre se ha asociado con algo más físico, con alarmas, con el vigilante de seguridad, pero yo lo asocio con algo más no con lo que tú has mencionado antes precisamente la visión holística. Normalmente estos conocimientos en materia de ciberseguridad e inteligencia no se adquieren en el Academia de Policía salvo en algunos casos de policías que provienen de unidades especializadas, información e inteligencia con lo cual me planteo cuál es el valor añadido que qué ofrece un policía.

Claro yo soy súper pro policía Además que tengo muchos amigos que son policías con los que me lía la guerra en inferioridad de condiciones además del compañerismo, la capacidad de trabajar en situaciones absolutamente adversas con muy pocos recursos y que tiene algún olfato que esto no te lo da ninguna carrera.

Algo parecido al médico que está en seguridad social y está viendo a centenares de pacientes. Quizás no pueda acceder a las mejores tecnologías, pero sí que se ha sabido hacer así mismo como un gran médico.

Últimamente se ha oído a hablar mucho del Big Data que se articula como el futuro en la inteligencia dada la capacidad que tiene de manejar cantidades ingestas información, ¿como ves tú el futuro Big Data?

Creo que es necesario porque la información ya está, con lo que si está mejor organizada nos vamos a beneficiar todos y cuando digo todos es todos los buenos y los malos y los que a veces han sido buenos y después han pasado a ser malos.

Ahora por ejemplo nos han invitado a ir a Estados Unidos y nos han pedido que cuáles son nuestras redes sociales preferidas. No es que no las puedan conseguir porque las pueden conseguir muy fácilmente haciendo un poquito de OSINT pero si empezamos a poner capas a la seguridad entre lo que te dan voluntariamente y la que tú estás pidiendo, más la información que esté en bases de datos que estén cerradas, diferentes tipos de privilegios en las bases de datos cerradas pues eso genera una capacidad de conocimiento que en la mente de una persona que la va a utilizar en positivo pues es que no tiene fin, es súper útil . A mí lo que me da quizá un poco más de miedo no es el uso que se vaya a hacer, que también, pero tecnológicamente todo eso cómo se va a gestionar porque ya me ha ocurrido de ir a un cuerpo policial, que tengan una súper idea de cómo van a poder utilizar el Big Data en su beneficio pero al final llega un momento que las tecnologías se quedan obsoletas entonces ponen una gran cantidad de dinero yo que sé 10.000.000 €, por decir algo, en una tecnología determinada y

después resulta que con Open Source podían haber conseguido las cosas. Entonces me da un poco de miedo que hay ahora como el gran estallido del Big Data y que empresas que se están forrando haciendo diferentes tecnologías y que el que toma las decisiones no sepa escoger bien cuál es la tecnología qué va a servir bien y en consecuencia no tenga cintura ni dinero para seguir implementándola.

11.2 Entrevista J.Nicolás Castellano

FICHA TÉCNICA	
Descripción	Entrevista a J. Nicolás Castellano, experto en Ciberseguridad, profesor de la Universidad de Barcelona y General Manager en Andubay.
Técnica instrumental	Entrevista semiestructurada
Objetivo	Extraer aquella información relativa a su experiencia en la empresa privada. Principales amenazas que trata, en qué departamento se ubica la ciberseguridad y por qué, el nivel de conocimiento percibido en la materia y nivel de implementación de las medidas de seguridad.
Fecha	14 de febrero del 2018
Lugar	Institut de Seguretat Pública de Catalunya.
Observaciones	

1.- ¿Podríamos decir que Ciberseguridad es tu especialidad? Cuál ha sido tu Ínterin hasta convertirte en un experto en la materia.

Mi camino dentro de la ciberseguridad empezó como un juego y empezó más como un juego autodidacta. Al contrario que mucha gente que se ha especializado por una necesidad de mercado digamos todos los que empezamos en mi ámbito empezamos como un juego ¿Por qué? porque éramos gente a la que nos gustaba la informática y principalmente lo que nos gusta es aprender sobre tecnología. Cuando apareció Internet, soy una persona que desde los 6 años ha tenido un ordenador, que ha pasado por distintas tecnologías hasta llegar al mundo de

Internet. Cuándo empezó el mundo de Internet sí que a través de un amigo me hizo descubrir otros mundos que parecían ser muy cómo te lo diría… hasta algo entonces inalcanzable. Internet en muchos aspectos abrió una veda en la que hubo días, noches, descontento de mis padres en la que empezó otra etapa de mi vida dónde empecé a ver todos los riesgos, todas las formas de hacer trampas en Internet. Más concretamente a través de páginas como la web del jamón y el vino que eran páginas que estaban en Isla Tortuga, eran páginas un poco que marcaban la rebeldía del mundo tecnológico. A partir de ahí empecé a ver qué había formas de hacer trampas en el mundo tecnológico y que podrían tener su trascendencia porque no olvidemos que cuando no existía Internet había gente que se saltaba las protecciones de los de los programas haciendo números de serie falsos copiando DVDs. Siempre, al final, detrás había otro submundo que era otro negocio que no era legal y que sustentaba esto. En aquella edad lo que nos movía todos nosotros era el aprender otras cosas y sí que todas estas páginas y todos estos cracks te daban otra visión del mundo que era el mundo que se veía. Hasta llegar a relacionarme con más gente porque a través de Internet pues la gente que estaba dentro del mundo del hacking del cracking del friki de una serie de técnicas en Internet estamos relacionados ya sea a través de una lista de correos de foros y digamos que en este panorama conocí a diversos actores que cierto día me animaron a … en un núcleo poblacional, Mallorca donde llegaba la tecnología, pero no había mucha gente especializada nos llevó hacer un congreso. A partir de ahí empecé a conocer, por eso digo que es un tanto diferente al mundo que se sigue, pero fue como llegué a la ciberseguridad porque de algo que era vocacional y autodidacta se convirtió en algo profesional, ¿vale? luego a través del tiempo se fue, todas estas inquietudes y esta manera de aprender que era un hobby se convirtió en algo profesional, al final esto llegó a ser una necesidad.

2**.- Cada vez hay más adicción a las nuevas tecnologías, sin embargo, el nivel de conocimiento de la sociedad sobre lo que hay detrás de ella, los riesgos que entrañan no van acompasados. ¿Cómo valoras esto, qué hacer para mejorar esta cultura?**

Hay un lema a un estigma que se están lanzando qué dice que las nuevas generaciones son las que están más preparadas tecnológicamente y de hecho yo estoy viendo cada vez más y de hecho en grados universitarios veo que hay poca gente que realmente esté preparada

tecnológicamente, hay más gente que parte de cero. esto quiere decir que la tecnología va avanzando es decir el negocio por una parte va llevando a las personas a que su adecuen a su mercado que es el mercado tecnológico y el de Internet y el de las tecnologías de la información y las nuevas las generaciones, coincido contigo, nos están adentrando en ese negocio en el terreno informático. entonces, ¿qué es lo que hay que hacer?, ¿qué es lo que sería conveniente para adentrar esa nueva generación al mundo tecnológico? De hecho, algunos ya lo están haciendo, darles una televisión les dan una Smart TV o una Tablet para que el niño ya se vaya entrando y en vez de darle un curso sobre cualquier otra cosa se lo dan sobre informática o manejo de esas tecnologías. Creo que es una cuestión que va a requerir tiempo lo cual juega en contra del negocio. Yo creo que forma parte el que se mejore … una de las cosas que yo haría en ese aspecto es que los colegios se de alguna asignatura desde pequeños. De hecho, ya hay algunas clases que ya lo están haciendo de cómo manejarse en las redes sociales y cómo utilizar bien las nuevas tecnologías. **Es decir, hacer un poquito de pedagogía de la seguridad que debe haber detrás la tecnología, ¿no**?

Exacto

3.- ¿Qué organismos nacionales e internacionales se articulan como referencias válidas en materia de seguridad?

A nivel nacional hay ciertos estamentos que nos ayudan a impulsar temas de ciberseguridad que creo que es a lo que te refieres. A nivel nacional tenemos estamentos como INCIBE que ayudan a la pequeña y la mediana empresa sobre consejos de ciberseguridad, luego también ccn-cert que velan por las Administraciones Públicas y que a nivel de Administraciones Públicas y algunas asociadas les da, les ofrece protección en materia de ciberseguridad como un servicio. A nivel por ejemplo catalán o a nivel andaluz hay ciertos cert que ofrecen un tipo de servicio pero en este caso están no como están como un órgano, no están como un órgano regulador sino como un órgano de auditoría en el que tú puedes contratar o no el servicio con ellos. Luego a nivel europeo existe también a nivel didáctico, de pruebas, ENISA, qué dentro del marco europeo es una agencia qué pautas de seguridad y tiene también sus cert especiales en cada materia. Tienen partidas presupuestarias para proyectos etcétera

4**.- ¿Cuál es tu valoración del camino recorrido en términos de ciberseguridad, dónde nos encontramos?**

Se están dando pasos, lo que pasa que lo que creo que hay que diferenciar dos tipos de organizaciones: la organización que por su nivel de madurez porque al final es un tema de madurez, como por ejemplo la banca que es una de las más maduras en temas de ciberseguridad porque uno de los principales alicientes para ellos es la propia imagen. A la banca le ha interesado que no se hable mal de ella que los clientes confíen en la banca entonces ha tenido que invertir siempre dinero, en materia de ciberseguridad para evitar fraudes y robos extorsiones etcétera. Entonces, yo destacaría un tipo de empresa que ahora mismo en su nivel de madurez está bien como por ejemplo es el de la banca y luego otro tipo de empresa que es el que está dando el salto a ciberseguridad. Ese tipo de empresa es una empresa que no se había planteado nada, ahora el espectro de atacantes es mucho más grande, el nivel de fraude, es mucho más grande, es decir todas las amenazas que hay en Internet se ha multiplicado los últimos años y como su nivel de implicación en tecnologías es tan grande, o sea dependen tanto de la tecnología, han tenido que adentrarse sí o sí en el mundo de la ciberseguridad, porque de hecho han tenido a nivel de negocio más perdidas qué años antes y han tenido que meterse de lleno en el mundo de la ciberseguridad. Lo que antes un administrador de sistemas informáticos escondía debajo de la alfombra porque desaparecía en algún momento dinero y no sabían de dónde pues había que buscar una explicación a eso, no han tenido más remedio que adentrarse en el mundo de la ciberseguridad. Podríamos diferenciar entonces estos dos sectores pero siempre hablamos de madurez.

5.- Dejando atrás el pasado, la siguiente pregunta tiene que ver con el futuro. ¿Cuáles son las tendencias y amenazas a las que nos tendremos que enfrentar durante el futuro?

Hay un tema principal que es, según el tipo de compañía. Empecemos por la pequeña. El tipo de compañía pequeña es una compañía que no puede invertir en ciberseguridad más de lo que va a perder, al final es un tema de negocio, es un tema estrictamente de negocio, es decir, si lo que puedo perder es más que lo que puedo invertir pues entonces ahí sí que empiezo en ciberseguridad si no, no me vale la pena entonces es como el que pone las videocámaras en supermercado y lo hace por un aspecto disuasorio más que por otra cosa. Esa compañía pequeña intentará dar el salto adoptando pequeñas medidas de seguridad, ya sea el antivirus, como otras medidas que le ayuden a paliar las amenazas. Después las organizaciones que empiezan a tener gran número de personal y que medianamente se van a ir adaptando en el plano Estratégico van a necesitar que la organización esté adaptada a unos procesos acorde

a unas buenas prácticas de ciberseguridad ya que no sólo a nivel físico a nivel procedimental van a tener que tener buenas medidas de seguridad sino también a nivel cibernético o informático . La mediana y la gran empresa cada vez va a tener que superar más retos de fraude y va a tener que superar más retos a nivel de nuevas amenazas o sea APT lo que nosotros llamamos Advanced Persistent Threat, que son amenazas que se conocen habitualmente, que pueden ser un tipo de ransomware o virus etcétera o la combinación de varias pero que se ha especializado para esa compañía. Como lo que tienes mucho que perder, bueno de alguna manera como los que vimos en las clases, lo importante es la información y la disponibilidad de los servicios y en esto la información es poder. Sí un mes de trabajo de un ciberdelincuente merece la pena o incluso de un equipo de ciberdelincuentes merece la pena realizar un ataque nuevo con una APT para una compañía entonces ese equipo se va a esforzar, esa banda organizada va a intentar conseguir esa información o tumbar los servidores o atacar esa planta nuclear etcétera

Es decir, nos enfrentaremos cada vez más amenazas más sofisticadas conocidas como APT, son amenazas dirigidas y también al fraude. Fraude como una de las principales amenazas.

Sí, estoy hablando a nivel de organización porque los usuarios tienen otras amenazas. Pero si me preguntas a nivel de organización las pequeñas empresas necesitan, porque las amenazas suyas van a ser recurrentemente ya sean randsomeare nuevos …. necesitarán de una industria para reforzar todo esto. Al final todas estas amenazas hace tiempo que existen lo que pasa que se está reforzando ahora mismo porque como hay más mercados digamos, todas esas empresas que están sometidas a la tecnología, los delincuentes tienen más mercado digamos. Entonces intentan sofisticar se ellos también o qué ese ataque llega la gran masa y esa gran masa están bien aquellas empresas que todavía no se han adaptado.

5- Qué es lo que más te demandan las empresas. ¿Dónde hay más carencias?

Una cosa es lo que nos dedicamos nosotros y otra cosa es lo que nos piden aquí también hay que diferenciar. Nosotros somos una empresa multidisciplinar pero sí que lo que nos piden mucho porque ahí somos buenos es en el tema de la formación. Las empresas grandes o mediana grande nos están llamando para aconsejar y formar a sus equipos de desarrollo y sus equipos de gestión. Es aquí donde tenemos gran parte de negocio. La otra parte es ayudar a esos equipos a realizar las buenas prácticas, es decir, sí el día de mañana van a implantar algún proceso ahí estamos nosotros para ayudarles. Es decir, mañana necesitan adaptar una web

nueva y que ellos no han podido securizarla como tal. Entonces hay un mercado que es el de las auditorías donde nosotros revisamos las aplicaciones instaladas en los sistemas y luego normalmente necesitan ayuda porque ya sea por tiempo o por recursos no pueden. O por desconocimiento, aunque esto es más es menos habitual, lo que pasa es que a veces no tienen recursos o tiempo para dedicar la parte de seguridad. Es un tema en el que los recursos ya están dedicados y en el que un equipo de personas no se puede doblar para hacer para hacer esta labor. Es aquí donde nos subcontratan. Luego hay otra parte que es la vigilancia, no quiero que suene mal este término de vigilancia, se trata de un tema de monitorización de los sistemas de ataques. Es otro de los servicios que demandan las empresas, es decir, el tema de monitorizar sus redes, ¿por qué? porque necesitan de alguien que les examine de todo aquello que no conocen para valorar si tienen que poner una contramedida nueva. Muchas veces tú tienes X contramedida y X software, pero no siempre las amenazas son las mismas en todo momento a lo largo del tiempo, sino que a lo mejor pues hay algo sobre todo en el tema tiempo, o sea muchas veces todas las empresas no adaptan sus sistemas en el mismo tiempo, sino que van por prioridades. Entonces las prioridades en ciertos ataques sobran negocio son las que prima y el resto de medidas ya serán después.

6.- ¿Cuál es tu interlocutor por antonomasia, dirección sistemas, departamento de seguridad?

Yo me encuentro de todo, todo lo que has dicho me lo encuentro director de Seguridad, gerencia, sistemas, aunque de hecho con los que nos sentimos más cómodos es con el director de IT o con el director de seguridad si lo hay. Pero muchas veces nos encontramos sobre todo en las empresas menos maduras las que no han dado el salto a ciberseguridad qué son personas que a lo mejor no estudiaron informática, pero les ha tocado el rol de Ti o de seguridad y que están en una posición en la que hay que traducir les muchas veces el lenguaje de la ciberseguridad a lenguaje del dinero.

Es un tema de entendimiento de hablar el mismo idioma.

Hay veces que sí que tengo que hablar con alguien técnico para decirle “un ping, un Dos”o lo que sea, pero hay veces en las que el director de IT ya no sabe lo que es una denegación de servicios, o le dices que un servicio se va a tumbar o que está tumbado. A lo mejor en este ejemplo concreto sí, pero si le dices si te hacen este ataque tus sistemas no van a estar disponibles durante 6 horas. Entonces aquí el director de IT sabe que, si sus sistemas están 6

horas sin funcionar, son 6 horas que en las en las que no puede producir, o que no está dando una visibilidad de su empresa. Pero, por ejemplo, hay ciertos tipos de ataque que si les dices qué un usuario o alguien mal intencionado va a robar su base datos o la va a modificar no se da cuenta del impacto que tiene en su negocio, es decir, hay que traducirle que, si me roban esa base de datos, si ese atacante tiene acceso para poder modificar sus datos, en su negocio puede ser que en lugar de vender las habitaciones en Hotel a 200 € la suite, la va a vender por 2 €. Entonces esto hay que explicárselo, o sea, no puede casar una cosa con la otra. A veces hay que traducirlo todo es lenguaje técnico al impacto en el negocio. Entonces desde mi punto de vista, al final somos como vendedores, como comerciales de ciberseguridad. Tenemos que darle nuestra visión de la ciberseguridad y luego riesgo por riesgo contramedida por contramedida qué es lo que le supone para el negocio. Porque como muchas veces cómo se hace un plan director, qué es decirle bueno, tú por tu modelo de negocio por cómo funciona, por tu manera de verlo, por tu estrategia, etcétera, vas a necesitar todos estos servicios, pero ahora yo contigo que eres el director de IT o el director de seguridad nos vamos a sentar para ver qué prioridad le vamos a dar a cada cosa porque al final no que manda es el negocio, a lo mejor el firewall será lo último que pongamos o lo primero depende de tu negocio

6.- ¿Dónde deben concertarse los esfuerzos de las empresas para blindarse?

Principalmente, aunque nuestra empresa es una empresa de medidas de seguridad reactivas, las empresas que están dando el paso para ciberseguridad o que tienen cierta madurez dónde deben centrar sus esfuerzos es en la dirección de los accionistas. Si estos son los que consideran que deben adaptarse y dar el paso a ciberseguridad y estos comprenden que a lo mejor, cierto riesgo, ciertas contramedidas de esos riesgos, como por ejemplo que todos tengan contraseñas que las contraseñas no sean un dos tres cuatro es ahí donde tenemos que ponernos.

Lo que acabas de Decirme llama la siguiente pregunta no I ES si el usuario es la principal amenaza

Claro el eslabón más débil es el usuario, y cuanto más poder tienes en un negocio pues más protegido tienes que estar. No puede ser que los VIP de las empresas o los directores generales no tengan contraseña o la contraseña sea el mismo login o ciertas prácticas que en tu casa no las harías. Estamos acostumbrados, qué estamos hablando del caso de España, dónde hay empresas dónde todavía hay imágenes de un señor con un puro la boca, que igual que dice

quiero esto para mañana, te dice que no quiere esa medida de seguridad o que le tienes que dejar navegar por cualquier página web o cualquier otra medida que pondría en riesgo la suda de su empresa. Repito que la información es el poder, es el capital de la empresa qué es una las cosas que hay que pensar. El capital, a parte del dinero que tenga en su cuenta bancaria es la información que maneja.

Es un tema de cultura de seguridad, integrar en todos los procesos de la empresa la seguridad, que la gente se conciencia con ciencia, que no dejen una contraseña en el posit pegada al ordenador

Básicamente aplicar todas las medidas que tú organización, a través ya sea de tu consultor o de tu director de seguridad o de la figura que tengas, que se tengan que adoptar; no todas las medidas de seguridad, pero sí que tiene que haber una escala de prioridades En las cuales algunas medidas mitiguen lo que afecta más.

7.- ¿Quién debería ser el interlocutor en el sí de una empresa para una profesional de la ciberseguridad?? ¿No crees que lo razonable sería que el Director de Seguridad fuera tu interlocutor?

Sí o no, depende de la estructura de la organización y me explico, Antiguamente informática colgaba de contabilidad porque se pensaba que la informática dentro de la empresa era un gasto y como era un gasto, un gasto de administración colgaba de contabilidad. Las siguientes estructuras pensaron que lo que era y IT o informática era un servicio más de una empresa y que si se contrataba fuera tenía un coste y se contrataba dentro tenía menos coste. Ya pasamos a la tecnología como parte de negocio, ya pasamos a otro escalón. Cuándo empezó a funcionar la figura de seguridad se metió por debajo desde informática, ¿por qué?, porque el que necesitaba seguridad era el órgano de ti. Pero seguridad no solo un tema estrictamente de IT, sino que es un tema de negocio, es transversal. Entonces depende de cómo lo mires la figura de seguridad puede estar en un sitio o en otro. Pero como yo lo vería en una estructura lo suficientemente madura es como uno más. ¿Por qué? Porque este interlocutor de seguridad lo que va a velar, él no va a dictar cuáles son las directrices en materia de seguridad de la organización, sino que según el negocio esa interlocución, lo que va a hacer es que con las demás figuras dentro de la organización va a consensuar cómo y en qué manera las va a adoptar.

Es decir, ¿te refieres a la figura la de un catalizador, ¿no? Es decir, va graduando todas las medidas teniendo en cuenta una visión corporativa. A mí a veces me da la sensación, quizás

por mi experiencia en un departamento de sistemas, que de alguna manera es como si una auditoría contable que la hicieras tú mismo. Es decir, introducir la seguridad dentro de departamento de sistemas da un poco está sensación. Puede dar lugar como tú has dicho, a que se escondan debajo de la alfombra cosas que no salgan a la luz.

Otra de las teorías que yo tengo es que el mismo desconocimiento que hay en la sociedad a nivel de ciberseguridad también se arrastra a los directores de seguridad que muchas veces son ex policías o personas que no tiene nociones de ciberseguridad como tal y qué les da miedo tocar estos temas y por eso se queda la ciberseguridad en el departamento de sistemas. Está habiendo ahora muchas decisiones que son a veces en el ámbito de la administración pública o en la privada qué es que antiguos policías, que los reciclan que no tiene la visión de ciberseguridad y que los meten en este espectro y que luego forzadamente porque no es un tema de vocación que se ven sometidos a entrar en el mundo de ciberseguridad. Ven la informática como un mundo de brujería porque hay aspectos inexplicables para ellos. En estos casos yo creo que lo idóneo es que está propia gente se recicle, y que si realmente es un tema de vocación o que les guste y tal entonces lo que deben hacer es aprender del mundo informático y también en materia de ciberseguridad; o alguna persona con conocimiento que venga por lo menos del mundo tecnológico. Hay una parte de la ciberseguridad que es, como es un tema tan amplio y como toca tantos temas, pues en la parte de gestión de riesgo, una parte que digamos la podría asumir alguien que no fuera tecnológico porque realmente con pocas nociones de informática o con medianas se podría medio solucionar. Pero hay otra parte que es la tecnológica que si no es alguien que está curtido en el mundo tecnológico es medianamente difícil curtirse o por lo menos lleva mucho tiempo adaptarse al mundo tecnológico y que sólo alguien que tenga vocación o que haya aprendido o venga de ese mundo que puede dar otra está otra visión, al final esta visión panorámica la puedes dar si tienes una parte tecnológica sólida, si no es muy difícil. Entonces contestando la pregunta depende del interlocutor, de su papel se puede hablar con uno o con otro hay cosas que se esconden debajo de la alfombra pero siempre, al final quién hace los que hacen movimientos de los organigramas está la dirección pero por encima está el consejo de administración y el consejo de administración se supone que son personas que dirigen sus empresas y que tienen que tener cierto nivel de madurez de sus empresas para poder decir que la manera que tienen para apostar

en ciberseguridad no sólo es con dinero sino poniendo al frente gente a cargo que domine el ámbito tecnológico y también de los otros ámbitos, del ámbito de ciberseguridad o por lo menos que haya tenido contacto con el mundo con este mundo.

8.- ¿Crees que hay una cultura de la seguridad en general en las empresas, ¿qué encuentras a faltar?

Al final todo, vuelvo a reiterarme, al final como las decisiones se toman de arriba para abajo y no de abajo para arriba hay decisiones que un empleado, aunque se diga siempre que en todas las organizaciones todo el mundo es importante, las decisiones no se toman de abajo para arriba puedes escalar, pero pocas son las que vuelven a bajar. Es de arriba hacia abajo desde un plano estratégico que la propia empresa a través de sus directores o consejos de administración se decide que haya esa cultura. Al final la cultura son medidas pero muchas veces entre esas medidas es esa cultura de toda la organización en ciberseguridad por ejemplo nosotros hemos dado para que se enriquezca esa cultura de ciberseguridad, formación a todas las a todos los miembros de la empresa, sesiones en las que se ven todos los riesgos y decirles que aparte de haber medidas legales que son las que te obligan la ley como la LOPD que te dice lo que tienes que hacer y que hay cursos de formación que también hay otras medidas en la que los empleados deben sentirse partícipes y tienen que saber que si te viene un email del banco no le clicques ahí. Son cosas que a veces la gente lo sabe, pero todavía pica. Aquí no podremos entender mucho porque la empresa se podría haber gastado mucho dinero en un sistema ransomware o lo que fuese, pero da igual…. hay algunos temas del usuario final que se traslada a la organización.

9.- ¿Qué porcentaje aproximado de empresas disponen de un plan de director de seguridad? De los que lo tienen, ¿cuáles hacen un uso debido del mismo?

El Plan Director de Seguridad se hace cuando no se van a implantar todas las buenas prácticas que una ISO como la 27001 te dice que hay que implantar. Entonces se hace o algo más pequeño que es un Plan Director de Seguridad dónde salen estos proyectos. Esta serie de proyectos estaba muy de moda antes, ahora cada vez está menos de moda porque, de hecho, las empresas empiezan a tomar la ISO como algo que hay que hacer, y se suelen adoptar esos procesos como si se tratara de otra o de cualquier otra y eso.

Creo que, a nivel de ISO, y a lo mejor me excedo en el término yo creo que la ISO tiene un carácter de imagen pero que si se cumple tiene una gran profundidad y un gran efecto en la seguridad. También lo otro que hay que comentar es que la seguridad muchas veces va relacionada con una falta de operatividad porque cuando más medidas hay más trabas y algunos procesos te hace más lentos.

Bueno de alguna manera es un poco comparable con el binomio de seguridad y libertad de encontrar el equilibrio entre ambas variables un equilibrio que te que permita avanzar a un ritmo normal.

10.- Cuál es tu valoración general de la figura del director de seguridad. ¿Cuál es perfil que te encuentras?

Yo me encuentro con todo tipo de perfiles pero es que depende de la organización con la que tratamos porque nosotros tratamos con todo tipo de empresas tanto empresas grandes las que tienen más madurez tecnológica y más madurez en cuanto a organización que tienen a un responsable seguridad y otras que no tienen tanto y tiene un responsable de IT que hace funciones de seguridad porque es el propio quién conoce los fallos que tiene pero no lo saca a relucir delante del resto de lectores porque no le interesa echarse m***** a él entonces yo creo que las que están suficientemente curtidas a nivel de organización ponen en esa figura un director más porque es un órgano independiente que a todos los niveles audita la seguridad de toda la compañía. Es en pro de la compañía no del mismo de su departamento. Aparte que el director de seguridad cuelga de TI es sólo de TI el otro es a nivel de organización.

11.- **Imagínate que mañana empiezas a trabajar en el departamento de seguridad de una gran empresa. Hasta la fecha no han hecho los deberes y no tienen implantadas medidas de seguridad. Por dónde empiezas, ¿cuál sería tu plan de acción?**

Es sentarme con el que manda y decirle. Bueno primero en la entrevista de trabajo yo lo que le haría es decir a ver qué es lo que piensa el de una figura cómo esta, si lo que tiene pensado es el niño que le va, el chico para todo, el que le va a arreglar todo entonces ahí voy a ver cuál es la mentalidad de esta persona que me va a contratar. Quiero decir, ¿qué me quiere como el becario que me va a solucionar todo a muy buen precio? o ¿qué libertad me va a dar para contratar proyectos de dentro hacia fuera y para vender? A l final uno tiene que ser un poco

comercial, ciberseguridad dentro de la compañía, y si hay presupuesto para gastarse y sino presupuesto en persona, cuál es la idea que tiene en la organización y ahí voy a ver.

Imagínate que no tienes límite, ¿por dónde hay que empezar?

Lo que hay que hacer es conocer el negocio ponerte al lado de las personas estratégicas y saber qué es lo que hay pensado hacia dónde va el negocio, en definitiva, cuál es el negocio de la compañía y después hacer a nivel de auditoría tanto de procesos de negocio cómo de medida seguridad, qué es lo que tiene hecho y ¿qué es lo que no tiene hecho? Si no tiene nada vamos a ver cuál es lo más importante y lo menos importante y a partir de ahí un plan de acción, a medio y largo plazo; a nivel de presupuesto asesorarme si puede ser desde dentro y desde fuera con empresas externas a ver quién me va ayudar a hacer todo esto. Luego pues saber, cuando cuentas con otras empresas externas a ver el nivel de madurez de cada empresa porque no es lo mismo una empresa que lleva 3 años no le voy a contratar lo mismo que una empresa qué lleva más tiempo. Depende de la madurez de la empresa le contrataré, a lo mejor a la empresa que lleva poco le contrato un pentest, ... en definitiva, ver un poco qué tipo de empresa es…

De alguna manera donde quería que llegarás es al conocimiento de los procesos como clave

Sí sí, al final hay que conocer la organización ya está te puede durar de 1 a 3 meses. No es un trabajo que sea fácil porque hay que ver la problemática que tiene porque va lento … por por muchísimos condicionantes. Tienes que estar dentro, que te diga el de más abajo por qué no puede hacer su trabajo, porque el otro día un accidente y no supimos nada …. Entonces hacerte una idea y cuando la tienes es informar y explicar cómo tienes la empresa a nivel de seguridad y ahora vamos a ver qué me dejas hacer de todo lo que hay que hacer. ¿no me dejas hacer nada? no es que yo creía que tú me ibas a hacer todo. Entonces a ver, ¿para que me contrataste? para hacer el chico para todo o para decidir cuál era el plan estratégico junto contigo. Al final yo decido cómo va a ir todo o al final es en el Comité de Seguridad donde se deciden las cosas.

11.3 Entrevista Carles Ortolà

FICHA TÉCNICA	
Descripción	Entrevista a Carles Ortolà, experto en Inteligencia, CEO Icaria Networks y profesor Universidad de Barcelona
Técnica instrumental	Entrevista semiestructurada
Objetivo	Obtener información de cuáles son sus principales demandas por parte de las empresas. Cómo valora el nivel de formación en su materia por parte de los departamentos de seguridad. Qué aporta la inteligencia a las empresas, principalmente en el área de seguridad.
Fecha	15 de febrero del 2018
Lugar	Instalaciones Icaria Networks
Observaciones	

1.- La primera pregunta Ocupó nuestras primeras clases del año pasado, pero me veo obligado a contextualizar el tema de la entrevista.

¿Qué es inteligencia y que no es inteligencia?

A ver, yo pienso que aquí las cosas son un poco difíciles de contextualizar, ¿por qué? porque sobre todo nos encontramos en lo que dice la teoría de los libros y cómo se interpreta la inteligencia desde este punto de vista, desde un punto de vista corporativo. Claro qué pasa, aquí en función de como sean los líderes, su bagaje, situación personal, de sus fobias interpretan la inteligencia de una forma a otra y esto es un gran problema porque no se contribuye a crear unas estructuras dijéramos homogéneas o que para entendernos todo el mundo hable el mismo idioma. Cuando dos médicos colegas hablan saben perfectamente lo que están diciendo y se ubican perfectamente unos con los otros; en nuestro caso no: a lo que unos llamar a inteligencia otros dicen que de inteligencia no tienen nada.

Pienso que para mí la inteligencia va más allá de la concepción tradicional. Al final no deja de ser un proceso de conocimiento un proceso epistemológico, en función de los inputs que

recibo. Tengo un problema necesito una información para tomar una decisión y actuar de determinada manera. ¿Cuál es la mejor forma de emitir de mitigar los riesgos en mis decisiones? Más o menos funciona si, así que necesito que el problema es que si yo tengo un problema por ejemplo me lo invento una ingeniería en la que tenga que diseñar un avión, hay una serie de problemas o retos de carácter ingenieril, de qué color voy a pintar las alas que herramienta voy a utilizar para poner determinado tornillo…. Claro, ¿esto es inteligencia? bueno en cierta manera sí o en cierta manera no. ¿Cuándo pienso yo que se puede hablar de inteligencia, de inteligencia más allá de los procesos y de retos internos de la empresa? Es cuando esto afecta dijéramos a la vertiente estratégica del sector. Por ejemplo, en el mismo ejemplo que te ponía de la inteligencia o de los problemas de ingeniería, sí el hecho de que yo utilice o una determinada tecnología o no la utilice, o a quién le compro esta tecnología y cuáles son mis procesos competidores de esta tecnología y no voy sólo a la parte dijéramos económica sino también política, sociopolítica, geopolítica, la que tú quieras. ¿Entonces aquí sí que hablaría de inteligencia, es decir, qué problemas resuelve la inteligencia en definitiva? No son problemas tan encajados en el día a día de las problemáticas sino las consecuencias que tiene desde un punto de vista integral de empresa o de organismo público en el caso público, del país o de lo que sea que haga que tú dijéramos tengas ventajas de cualquier tipo. Es decir, es una forma de mitigar riesgos conociendo la información. Y, ¿qué tipos de riesgos? tú te enfrentas a riesgos de carácter reputacional, de carácter estratégico, de carácter económico, pero siempre desde un punto de vista holístico. yo pienso que aquí está la principal diferencia.

2.- Si nos centramos en la inteligencia, ¿de dónde venimos, ¿dónde estamos y dónde crees que vamos?

¿En España? **Este caso si el ámbito de estudios España.**

Venimos de la nada precisamente por lo que hablábamos antes. Ha habido hasta ahora y esto se puede extrapolar por un lado a la parte pública y a la parte privada. Venimos de un mundo muy medieval en este sentido donde supuestamente hay una serie de, o había una serie de gente que a priori hasta hace a lo mejor 10 años no sabían lo que era la inteligencia, en las que también habido unas relaciones de maestro y aprendiz y esto es así. Tenías al típico policía, al típico Guardia Civil y al típico espabilado de turno que, en algún momento, intentaba solucionar los problemas de las empresas o de los sitios donde estaba asociado des de un punto de vista

totalmente tradicional, basado en su libre albedrío: yo creo que se le va a hacer esto y vamos a solucionarlo así. Esto es poner parches a las cosas. Siempre hemos tenido una tradición muy reactiva y lo voy a solucionar con mis amigos de la manera que yo pienso. ¿Qué pasa? Que esto hace que no hubiera ni método ni una altura de midas mara decir hemos de llegar aquí. Claro, en el momento, siempre aquí en España, que las corrientes anglosajonas, sobre todo impulsadas por las multinacionales, y podemos hablar de bufetes de abogados empezamos a incorporar términos como la inteligencia o inteligencia económica o compliance etcétera, de repente se encuentran las estructuras que habían aquí creadas, insisto medievales, y totalmente de reino de taifas, necesitamos adaptarlas a un sistema, a un vocabulario a unas concepciones a unos conceptos que son estos los de la inteligencia no tanto porque ellos lo quieran sino porque vienen impulsados por la propia coyuntura global. Las empresas necesitan más esto. ¿Qué pasa? Que al final hace que esta gente ha continuado haciendo lo mismo que estaban haciendo y simplemente han cambiado la etiqueta. Si yo antes tenía un problema y quería saber, me lo invento, sí tenía un problema con un proveedor iba y le partía las piernas, muy barrueramente, es muy así, pero a lo que a lo que antes decía le voy a darle dos hostias ahora le llamo inteligencia. ¿Qué ha pasado? que esto desde un punto de vista también privado han comenzado a ponerse en pelotas estos conceptos. Y mucha de la gente, insisto que venía ejerciendo estos cargos le ha cambiado la etiqueta y por otro lado han salido un cúmulo de gente que se ha apuntado a este a este carro a esta moda. Te pongo el ejemplo por ejemplo de detectives privados o incluso policías. Son gente que heredan unas formas de hacer, que muchas veces no tiene nada que ver con la inteligencia, y que hacen cosas que …ellos confunden la parte con él todo. A lo que ellos llaman la inteligencia esto, perdona, es simplemente un input más que no tiene nada que ver con el concepto. Claro, ¿qué pasa?, que de repente te encuentras con más problemas todavía.

Precisamente porque cada uno ha tenido que adaptar su lenguaje al imaginario colectivo más o menos influido por las películas que ha visto, de los libros que ha leído o por las personas con las que se ha relacionado te dirán que la inteligencia es una cosa u otra.

¿Pero base científica poca no en este caso?

No, absolutamente no. Uno de los principales retos que hay y que se está promoviendo es que al final el sector un poco lo que tiene que intentar hacer es limpieza, en el buen sentido de la palabra, en el sentido de reciclaje. Hay que determinar cómo se hace esto, con qué herramienta

se hace y sobre todo ser capaces de unir o de crear un discurso común que permita evaluar mutuamente, como lo que hacen los médicos que se evalúan unos a otros. Aquí también tenemos que avanzar en el mismo sentido.

3.- Háblame de ti, ¿cuál ha sido tu recorrido hasta llegar donde estás?

Yo cuando comencé en este mundo qué hará unos 5 o 6 años acabé de rebote mi background es de ingeniería, muy influenciado por la parte de procesos y procedimientos, de crear un corpus de conocimiento común que nos permite avanzar y acabé así. Estaba en Londres y haciendo búsquedas en Google en el mundo del análisis (en aquel momento pensaba que se trataba de las películas típicas y tópicas). Una vez comienzo a profundizar en estas temáticas, aquello que estás haciendo es algo tan genérico que tendrás estos problemas. Yo siempre lo digo, siempre pongo la misma coletilla: para mí la inteligencia es un proceso de crear conocimiento un proceso epistemológico es una disciplina absolutamente igual a la filosofía (cogido con pinzas). Cualquier tipo de filosofía, matemáticas, ciencias sociales, es igual, para mí sería parte aplicada de cada una de todas las disciplinas juntas. Luego hablaremos de la multidisciplinariedad. Bien, acabo así y tenía muy claro que hacíamos nosotros. Mi lucha siempre ha sido la misma: necesitamos poner nombre y apellidos a nuestro trabajo a decir lo que es y lo que no es. Necesitamos marcar unos estándares. **Por ejemplo, ¿al artículo que escribiste la inteligencia no es una tostadora?** Exacto siempre lo tengo claro, me lo planteo incluso empresarialmente, desde mi propia empresa. Tú tomas decisiones en función de la información. **También es lo bonito no de la inteligencia entrar en un mundo que no conoces y generar conocimiento** Exacto, tal cual, por lo tanto, es aquí donde me ubico yo. A mí el hecho de ser un experto de … dijéramos en cosas muy concretas al conocimiento no de conocimiento sino de la obtención del conocimiento no me interesa desde mi óptica porque sí yo necesito en un momento X tener un experto en plantas del Sahara me lo busco. Pienso que la capacidad o dijéramos el final último de la inteligencia es el de aglutinar conocimiento totalmente diferente. **¿Te refieres a Desgranar todo el conocimiento?** Exacto hacer un puzle de las diferentes cosas

Servirle esta información al cliente y que él tome sus decisiones, ¿no? Exacto exactamente aquí está siempre la eterna discusión, dicotomía de ser un experto o un generalista. Mi punto de vista es que dijéramos la inteligencia como ciencia tiene que ser lo más generalista posible porque precisamente cuando tú necesitas más mano experta en alguna temática ya sea en una temática

o en las formas de obtención o en lo que sea, hay gente especializada en esto por esto a esto no hay que decirle inteligencia es a donde quiero ir esto es una parte más del todo.

4.- La inteligencia siempre se ha asociado a los servicios secretos, a la seguridad pública y cuerpos de inteligencia. Empieza a haber negocio en la empresa privada, ¿cómo se ha ido gestando esta colaboración en la parte privada?

Es lo que te comentaba antes, Me baso en mi experiencia vital no tengo más elementos que estos Y habría casos en los que sería puntual y la norma no aplicaría. No sé hasta qué punto la norma aplica o no. Nace sobre todo por el concepto que te comentaba antes. Sinceramente, pienso que no existe este sector. No existe como tal, existen partes muy puntuales parte muy sesgadas, no en un sentido malo, sino muy parcial. Sobre todo, fruto de la herencia inicial de este modelo antiguo tradicional se han visto forzados a cambiar el método. ¿Hasta cuándo durará esto? Sinceramente pienso hasta que se mueran los que están llevando la inteligencia, tal cual. ¿Por qué? aquí sí que es verdad hay una parte muy importante, es un poco complejo todo esto, pero desde un punto de vista dijéramos "in house" de las grandes compañías internas, se da incluso este paradigma o esta paradoja. Todo y tener supuestamente la información asociada a los sectores o a las divisiones de seguridad esto está cambiando y eso está cambiando porque se dan cuenta de que las necesidades de información cada vez más, y sobre todo cada vez más las multinacionales porque es donde más dinero hay para hacer esto, dijéramos no pasa por articular desde un punto de vista de seguridad. De hecho, las iniciativas de inteligencia corporativa que hay actualmente pasan más por asesores personales de la alta dirección que no por centralizar lo en un in House en temas de seguridad o departamento del departamento típico de seguridad. Yo sí que concibo o me doy cuenta de que cada vez más son menos las reuniones con los departamentos de seguridad porque personalmente, incluso a mí, no me interesa porque te ven como un competidor de su trabajo cuando realmente no tiene nada que ver con tu trabajo. Y sobre todo por este cambio de paradigma, es decir, la inteligencia no puede ser utilizada como una herramienta reactiva tradicional de la seguridad. Tiene que ser vista como prevención y sobretodo como estrategia. Deja de tener sentido desde un punto de vista de la alta dirección de las empresas llevar la inteligencia desde los departamentos de seguridad, y pasa a tener sentido llevarlo desde los departamentos de estrategia o estratégicos. Dependerá

mucho de la organización de las empresas porque hay veces que el departamento o el Director de Seguridad sí que tiene voz y voto en el Consejo de administración, pero la gran mayoría no, pasa más por los consejeros o director ejecutivo de las empresas. Esto y acabo, donde nos lleva es que haya empresas como las por ejemplo DELOITE, CAPMG, tengan mucho recorrido porque ellos no tienen el estigma. Al final piensa que estás empresas son como verdaderos entes de inteligencia propios. Con tentáculos en todo el mundo tú coges un Deloitte y si quieres información estratégica del Perú tranquilo que llamarán a su socio del Perú y la tendrás en un momento. Por lo tanto, fíjate que hay una doble velocidad: por una banda tienes una gente que supuestamente dice que quiere hacer inteligencia, pero no tiene los medios la capacidad de acceso a las altas esferas de dirección, que toman las decisiones y sin embargo se empecinan en decir que hacen inteligencia; en cambio tienes otra gente que realmente está aportando valor en toma decisiones, que ellos nunca dirán que están haciendo inteligencia ellos dirán que están asesorando por lo tanto es aquí. Por un lado, estos quieren utilizar esta etiqueta para promocionarse y los que la tienen no la quieren hacer servir porque es que dicen que son asesores del presidente.

Esta concepción no lo había pensado, pero me parece muy interesante y de alguna manera me estás contestando a la siguiente pregunta. Ahora nos centramos en la seguridad corporativa y entendamos corporativa como mediana o grande empresa ya sea un banco…. ¿tienes tu interlocutor por antonomasia?, normalmente, quién es tu interlocutor, ¿con quién hablas, ¿con quién te reúnes en este tipo de empresas?

Todo depende del tipo de empresa y obviamente del tipo de filias personales de la gente, todo depende de la capacidad de acceso que tú tengas. depende de muchos factores y tradicionalmente mi interés desde un punto de vista de empresa privada, a mí no me interesa un director de seguridad, no me interesa para hablar con un director de Seguridad. A mí me gusta hablar con el CEO de la empresa, ¿Por qué es? porque yo sé que le puedo aportar un valor añadido y además me pasa una cosa muy curiosa. Mi experiencia me dice que todo aquello es, que todos aquellos proyectos que hemos desarrollado a través de los departamentos de seguridad no acaba funcionando y te va a explicar por qué. Fíjate que una de las cosas más importantes en nuestro sector es que tú tienes que hablar siempre con el interlocutor adecuado y el interlocutor adecuado siempre pasa por saber quién va a ser el usuario final de esta información. Si tú, desde un punto de vista estratégico atiendes una serie de peticiones, si tú

no tienes la interlocución directa con quién va a utilizar la información y con quién la va a recibir especificándote qué tipo de necesidad de información exactamente quiere estás abocado al fracaso, ¿por qué? no por nada por lo del telefonillo loco. Es muy fácil que la información se filtra interesadamente por ciertos interlocutores. Muchas veces tampoco es así. el gran problema es que si tú no tienes el interlocutor directo para que tú le puedas preguntar sobre sus necesidades y cómo se pueden alinear tus servicios con sus necesidades estás condenado al fracaso.

A Lo mejor lo que puede estar pasando alguna vez es que el mismo departamento de seguridad sea una especie de elemento inhibidor del CEO que a veces no se le daba toda la información o simplemente éste la filtra en base a sus propios intereses.

Exacto, aunque a veces no tiene porqué ser así siempre.

Ya, pero a veces pasa, Supongo que depende de la cultura la propia empresa.

Exacto al final a los departamentos de seguridad de empresas fruto de de esta gente que ha estado tradicionalmente en este sector (se refiere a la policía) tienen una actitud muy protectora.

Es que a lo mejor esto es un tema desconocimiento. Yo siempre he dicho y me baso en mi propia experiencia, cada uno tiene la suya, … cuándo encuentras una persona que quiere aferrarse a su silla es porque es muy insegura, que es fruto del desconocimiento. Igual es lo que está pasando aquí en este en este ámbito.

Además, te encuentras, e igual me estoy aventurando en exceso con esto porque a lo mejor mi experiencia no es tan extensa en esto. Pienso que los relojes generacionales que se están produciendo en las grandes multinacionales, o en las grandes empresas, incluso en las medianas empresas, me es igual, pasa porque antes siempre había el señor de toda la vida, teniendo en cuenta que las empresas grandes son de segunda y tercera generación, en las que te encontrabas el señor que hizo la fortuna y tenía su persona de confianza al lado que normalmente evolucionaba para hacer el Departamento de Seguridad y si no se incorporaba en él. Este era el típico que decía tú tranquilo que me encargo yo de todos los problemas. ¿Qué ha pasado?, qué ha llega el hijo u otra gente que por ejemplo ha estudiado en Harvard y claro acaba llegando a ser el presidente. Se produce una dicotomía cronológica clara que ni ellos mismos entienden. Se cuestionan, como este señor va a proteger mis intereses, de las inversiones en Argelia, ¿qué coño sabe este señor?, ¿qué solución tiene este señor? Este señor que venga aquí

y que vaya haciendo cosas, pero los problemas estratégicos yo los dirimiré con mi gente. Se sienten más cómodos hablando con Deloitte porque hablan el mismo idioma que no con un señor de la Policía de la Guardia Civil o donde sea porque estos no hablan el mismo idioma.

Sí que es verdad que hay corporaciones que tienen amenazas reales en temas de seguridad, aquí sí que sería lógico que, en esta parte, el Director de seguridad o el Departamento de Seguridad tenga mucho que decir

Y tanto, y la suele tener, y generalmente se relaciona con temas internos, recursos internos.

Yo sinceramente pienso que actualmente al margen de sectores muy puntuales, por suerte o por desgracia un banco, problemas serios de entidad física, entendidos como se seguridad tradicional, son muy mínimos. Actualmente las amenazas no pasan por aquí, por esto. Actualmente lo que más le preocupa a un banco es una OPA n Angola o que cambie el presidente de turno de Shanghái. estas son las verdaderas amenazas que tienen hoy en día en las grandes corporaciones.

Lo que sí que veo que cada vez hay más especialistas de seguridad contratados en los departamentos de seguridad de las empresas. Esto puede ser debido a la falta conocimiento del director de seguridad por ejemplo en materias de inteligencia.

Nada que ver con esto, es un tema de moda, y además me hace gracia esto porque sí desde estos sectores qué dicen que son inteligencia, ellos lo ven como gente de su propio gremio, pero lo que realmente están contratando no son gente de este sector, son analistas de datos científicos de datos, son informáticos, son matemáticos, son filósofos, son este tipo de gente y ¿por qué? Por la explosión de OSINT, por ejemplo. Tú necesitas este tipo de gente experta por ejemplo ahora mismo, experta en obtener cantidades ingentes de información que al mismo tiempo pueda ser analizada por un programa interno que te permita analizar en tiempo real cuáles son los movimientos de hashtags que haya por ejemplo dentro de una empresa en temas reputacionales, ¿qué pasa? Que toda esta gente tan especializada en conocimiento técnico únicamente los pueden liderar técnicos porque la otra gente no se entera con esta gente, no saben explotar su potencial y esto la alta dirección no tiene muy claro por esto si te das cuenta los currículums del Ibex 35 de los consejos de administración y de los altos cargos directivos cada vez más son ingenieros y eso pasa por esto. Al final es un tema de lenguajes y como un director de estrategia o de operaciones de una empresa sabe que esto de la seguridad está muy bien, pero lo que a mí me da dinero es tener gente con 50.000 pantallas o 52.000 ordenadores en una

habitación, que puede ser más útil o puede ser menos, pero es esto lo que ellos quieren y esto es lo que es útil según ellos. Por lo tanto, claro, esto de que estén contratando unidades de inteligencia no está tan claro, están contratando a científicos de datos.

¿Inteligencia y ciberseguridad convergen?

Cada vez más y cada vez más porque de alguna manera relacionada con la pregunta de antes, fíjate que es muy paradójico, porque la gente de seguridad cada vez tiene su ámbito más restringido, ¿por qué? Porque su carácter dijéramos generalista está jugando en su contra. Las principales amenazas, y sobre todo también en altos niveles, que tienen las corporaciones son por un lado los temas de espionaje industrial, los temas de ciberseguridad, de que alguien se meta dentro de que consiga información de mi interior y, por otro lado, de carácter estratégico o estratégico económico. ¿Qué es lo que pasa que si uno de estos problemas por ejemplo en el caso de Nike es que hackeen mis servidores y me hagan caer el negocio? hace que yo necesite expertos en esto, que yo necesite evaluar mis amenazas. Pero para evaluar esto necesito conocimiento y muy técnico. Un director de Seguridad entendiéndolo como la figura actual del director de seguridad no es capaz de esto. Y no porque tenga nada en contra de ellos sino porque el mercado ha evolucionado hacia la tecnificación y al final necesito gente analista que sea del gremio de la gente que esté contratando porque si no nunca en la vida podré extraer el máximo potencial y alinearme con esta gente e ir en la misma dirección.

¿Crees entonces que la lógica nos diría que el perfil del director de seguridad tiene que romper con el modelo tradicional El modelo que normalmente, y para mí desafortunadamente cuelga de un policía?, ¿debería evolucionar hacia un perfil más técnico?

De hecho, si miras planes de estudios te lo del mundo anglo Sajón hay masters en seguridad, gestión de crisis gestión de emergencias donde el 60% pasa por entender técnica computación entender un algoritmo. Cada vez menos planes de autoproteccion menos papel menos protocolo muchos de ellos anticuados y mucho más conocimiento generalista técnico especialista.

La siguiente pregunta tiene que ver con las comunidades de inteligencia que cada vez hay más que son, ¿que nos aportan?

Depende de la temática. Como al final la inteligencia abraza muchos temas dependerá del tema que trate. No existe una comunicad de Inteligencia de Inteligencia propiamente dicha.

Sí que es cierto que empiezan a crecer las comunidades y te encuentras con que existen dos o tres tipos de velocidades diferentes. Por un lado, te encuentras con un agente donde yo me encuentro. Yo busco la tecnificación de la inteligencia precisamente por este paralelismo qué está pasando con el mundo de la seguridad, qué está haciendo que nos estemos quedando a remolque de las cosas y al final acabe siendo un paria o un reloj antiguo. Pero hay comunidades muy potentes con temas muy específicos como por ejemplo terrorismo y crimen organizado o prevención de delitos, y por otro lado está la comunidad más técnica tecnificada en cuanto metodología, protocolo o en cuanto a lo que sea o en cuanto a concepción de inteligencia.

Que haya una cúspide que conozca todo esto, no existe. existen reinos de taifas. También está la parte tradicional formada por eruditos que van discutiendo sobre el sexo de los ángeles, ¿no?, pero comunidades de inteligencia de inteligencia no existen.

Pero yo pienso que esto es bueno porque es fruto de la evolución natural de esto es un planteamiento mucho de Darwin. Aquellas comunidades que sean capaces de adaptarse sobrevivirán y aquellas que no seguirán haciendo conferencias y no sé qué, que estará muy bien hasta que se haya de utilizar.

Se puede dar el caso de que una información considerada como reservada en nuestro territorio, pero no es reservada o se puede tener por la vía de otro país y puede llegar a través de las unidades de inteligencia antes que la propia policía es decir se puede dar el caso en el que, las empresas tengan información de primera mano antes incluso que la policía

Siempre, en en el 90% de los casos, pasa por muchas cosas, en primer lugar por la burocracia, cuando entramos en el sector público entramos en los grandes en los grandes elefantes, es como un todo siempre, hay un mastodonte que hay que alimentar y hay un montón de …, poniéndome en la óptica pública, como policía para poder acceder a no sé qué, tengo que rellenar 72 formularios, no sé cuántas firmas y obviamente tengo que tener los recursos y esto alineado con las políticas y las decisiones del gobierno de turno. Finalmente tienes que pelear, … y cuando acabas de pelear te resulta que ya ha pasado el problema. ¿Qué pasa desde un punto de vista privado? Pues que es muy muy mucho más ágil y sobre todo por lo que te comentaba antes, y me alejo del departamento de seguridad como tal. Desde un punto de vista estratégico CEO, si tengo un problema llamo a CAPMG porque sé que me conseguir a esta información por sus tentáculos en todo el mundo. Al final es un tema de eficiencia y es la eficiencia la que funciona en el mundo privado. Aquí para que un policía consiga una

información que venga de su compañero de Nantes esto puede suponer la tira de tiempo para conseguir esto, En cambio el de Deloitte llama a su compañero de no sé dónde y le dice dime esto cómo está y en 5 minutos la tienen esta información. al final es un tema burocrático 100% en este sentido.

Desde un punto de vista de la seguridad o directores de seguridad o de problemas tradicionalmente asociados a ésta, también pasa lo mismo, es decir, gente que tiene contactos en muchos sitios.

Incluso policías de otros países donde esta relación público-privada este más desarrollada , o sencillamente que las barreras que se encuentran aquí no se encuentren otros lugares, entonces si esto es así Y me viene perfecto para formular la siguiente pregunta cómo afecta esto la relación público-privada Si venimos de un mundo en el que la seguridad privada tal y como dice la ley está subordinada a la pública y está relación después de la ley del 2014 se intenta equilibrar de iure aunque yo creo que no de facto, ¿Cómo afectará esto a la relación, sí la información es el poder y yo tengo la información , ??

Aquí varias cosas: en la relación pública-privada la norma general es que no existen. España va muy retrasada, el sector público es muy hermético, muy receloso se su negocio a priori justificado por sus temas sensibles. Esto en Estados Unidos hace mucho tiempo se dieron cuenta de que gestionar millones de kilómetros cuadrados es imposible, pero se dieron cuenta de la idea de que 22 ojos ven más que cuatro, aparte de las capacidades económicas mías como gobierno nunca van a ser tan completas como las que puedan tener las grandes empresas. Haciendo un paralelismo lo que pasa aquí con la sanidad pública en la cual yo como estado no me puedo hacer frente a según qué inversiones.

En este sentido la colaboración en España no existe y no se espera que exista, pero más allá de esto vamos a hablar de la Ley de Seguridad Privada. Creo que es la última estocada que le faltaba al sector de la seguridad privada en España y te lo explico es muy sencillo. ¿Qué te impide a ti consultora estratégica asesorar a tus clientes? ¿Qué necesito para asesorarlos? ¿Si tú necesitas saber dijéramos cuál es la acción qué hay que hacer para ganarme al accionista de Sri Lanka que necesito con esto? pues tener información sobre esta persona. ¿Qué me impide mi hacer esto si esto es mi trabajo? Antes de tomar la decisión de cómo voy abordar a esta persona me tengo que informar sobre ella. De la misma manera que cuando lleva informes de la evolución del mercado de la madera en Colombia necesito información sobre Colombia sobre la madera en

Colombia. Pero claro desde un punto de vista de las empresas de seguridad resulta que la ley me está diciendo qué no puedo hacerlo. Sólo puedo hacerlo si pongo este conocimiento en manos del Estado es decir si le digo lo que estoy haciendo en todo momento lo que está haciendo el Estado es fiscalizar restringir cada mes cada vez más la capacidad que puedan tener los departamentos de seguridad.

Por esto yo pienso que lo que está haciendo la Ley de Seguridad Privada es blindar esta relación de subordinación, Por mucho que diga que es de igual a igual

Y tanto, y tanto. La finalidad de esta ley es la fiscalización completa de lo que se está haciendo en el país. Desde un punto de vista lógico esto tiene mucho más fácil solución y es estableciendo las colaboraciones público privadas; ahí sí que te aseguras de tener gente trabajando para ti y sabrás lo que está haciendo en todo momento.

Estas cosas por ejemplo en un bufete de abogados, claro que necesitan información ¿cómo van a hacerlo si no? esta gente está exenta de todo esto, ¿tú me has de fiscalizar a mí? no me afecta la ley y estoy haciendo lo mismo que hacen estos. Por lo tanto, esta ley es una ley anacrónica y no sirve para nada más allá de hundir todavía más el mundo privado de la índole que la que te estaba hablando.

Pues dicen que el reglamento que va a desarrollar esta ley va a ser mucho peor y que va a pretender fiscalizar mucho el sector privado

Claro, aquí es como siempre, los lobbies se preocupan de frenar estas cosas, pero ¿Qué fuerza podrá hacer un lobby de los detectives privados? ninguna absolutamente ninguna.

Últimamente se habla del Big Data, a priori es una poderosa herramienta para captar inhumanas cantidades de información. ¿Esto no es contraproducente para lo que es la inteligencia? ¿es el futuro de la inteligencia?

Sólo es una parte más de la inteligencia.

El problema del Big Data pasa en cierta manera como lo que ha pasado con el punto COM, hay un gran BOOM, a todo le llaman Big Data y todo no es Big Data. Al final el futuro de esto es que se deba estabilizar y se ponga donde tiene que estar con el paso del tiempo. El término Big Data hasta hace poco estaba en boca de todo el mundo y ahora se habla de la inteligencia artificial que es el siguiente paso, es decir la selección automática de la información en función de mis intereses. Todo Esto está muy bien, pero al final yo quiero sacar conocimiento, Y esto no aplica aquí. qué pasará? que con el paso del tiempo la tendencia a esta huida hacia adelante del sector

de la seguridad, de la inteligencia, dile como quieras, al final acabará siendo una parte más cómo puede ser el OSINT, Humint Al final el Big Data será una parte más del OSINT, y será una parte fundamental como el Humint. Pero insisto, está muy lejos de que las empresas, o del sector de seguridad (la inteligencia no está en el sector de la seguridad, sólo una parte). Por lo tanto, Acabará siendo una fuente más de información, al final veremos cómo trato esta información Aquí volvemos al punto de partida de siempre, para saber lo que quiero o que le puedo exigir a cada parte de estas necesito a gente que hable este idioma. Fíjate que al final exige que como experto en inteligencia tienes que ser experto en muchas cosas. No experto experto, sino saber conectar con el lenguaje de cada una de las patas que yo estoy tocando. Claro esto, tal como se enfoca en los estudios, lo acaba asumiendo gente especialista, y se acaba montando equipos de esto esto y esto liderados por un director de proyectos, y se aseguran de que todo el mundo habla la lengua de todo el mundo y se ponga en común el conocimiento y este es el futuro. Sí una empresa quiere especializarse, que se olvide de la seguridad como sector holístico, tiene que contratar a gente experta en cada una de las patas que quiera desarrollar y contratar a un director de proyectos que lo lidere. Esto es lo único que se ha de hacer. La respuesta que puedan dar los sectores de la sociedad corporativa cada vez será más obsoleta y cada vez servirán para menos y acabarán donde no quieren acabar donde precisamente no quieren acabar, poniendo un segurata detrás de la puerta.

Pero esto es fruto de La mala praxis que está haciéndose, Es decir, no concibo departamento de una gran corporación sin un analista o un generalista dentro de su unidad que conozca el idioma de la inteligencia

Si está figura es fundamental y de hecho Insisto sí que hay corporaciones que lo están articulando bien. Yo me refiero más al ideario colectivo que hay detrás de esto, que al final se traduce en qué tipo de gente por ejemplo incluso voy más allá incluso al tipo de gente que se matrícula en un grado de seguridad por ejemplo la seguridad cada vez más se está enfocando a técnicos a gente que tradicionalmente no estaba en este sector, pero esta gente es la que está aportando el valor a todo esto. Tú imagínate que en un grado de seguridad entendido como como esta pieza clave dijéramos generalista, por matemáticas tú en cada promoción tendrías que tener 7 personas, porque no puedes dar salida a todo esto no tienes 272000 empresas que necesiten este tipo de figuras. Claro, ¿Qué pasa? que también van en función del nivel de expectativas que tenga cada uno de los que entran en este mundo de la seguridad. Hay gente

que se sentirá muy cómoda insisto, poniendo un guarda de seguridad en la puerta y se sentirá muy bien haciendo esto, siendo responsable de esta labor De aquí a modernizar esto, a querer poner los departamentos de seguridad legítimamente en el sitio que la gente del sector de seguridad diga que se merece es muy complicado. Esto no es una crítica, ni mucho menos, lo que quiero decir es que o espabila el sector y de verdad pone gente que de verdad pueda dar soluciones a los problemas porque cada vez más los departamentos de seguridad de las empresas no van por libre, no pueden hacer lo que quieren hasta ahora iban haciendo y deshaciendo más o menos como ellos querían. Ahora no pasa esto, ahora tienes un presidente o un CEO que ha estudiado en Harvard y no le cuentes milongas, ni historias porque muchas veces su problema es saber si los de Siberia van a comprarme o van a hacerme alguna guarrada.

Bien y la última pregunta ya me la has contestado más o menos y es que qué es lo que encuentras a faltar o qué es lo que echas de menos en las en los departamentos de seguridad de las empresas, que supongo que es que se hable este lenguaje al que hacías referencia antes, un lenguaje técnico EXACTO

La otra cuestión tiene que ver con haber si hay conocimiento por lo que respecta tu materia, que ya me has contestado que no.

Aquí yo principalmente lo que veo es un cambio en la organización es decir pasar de estructuras verticales e impermeables a unas estructuras horizontales, pero no estructuras horizontales para que quede bonito sino porque realmente necesitas esto porque sino no vas a ser capaz de solucionar ningún tipo de problema.

11.4 Entrevista Juanjo Cantero

FICHA TÉCNICA	
Descripción	Entrevista a Juanjo Cantero, Director de seguridad corporativa grupo CBRE.
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector
Fecha	19 de febrero del 2018
Lugar	Instalaciones CBRE Diagonal Mar
Observaciones	

1.- Juanjo, seguramente seas una de las excepciones que rompe la regla, en el sentido de que según tengo entendido empezaste de "0" en el mundo de la seguridad y has llegado a ser director. ¿Cuál ha sido el recorrido?

Bueno pues el recorrido ha sido largo y tedioso. Yo empecé, el primer contacto que tuve con la seguridad fue en el ejército, estuve 3 años y a partir de ahí se despertó un poco la sensación de que el mundo de la seguridad iba a gustarme, y los inicios fueron, … yo dejé el ejército en el año 88 y ese mismo año comencé un curso de lo que antes era denominado guarda de seguridad. Aquí fue cuando recibí la primera formación que además será una formación subvencionada por el INEM y una vez que lo acabé entre en el mercado laboral, anteriormente no había hecho nada excepto el ejército y algún plan ocupacional que hice de joven, con lo que mi entrada en el mundo laboral fue en el mundo de la seguridad y ahí empecé como todo el mundo empezó, de guarda. Luego además en aquellos tiempos tenías que esperar a los 21 años para para ser vigilante jurado porque para aportar arma la ley decía que tenías que ser mayor de 21 años. Y así estuve hasta que realmente me hice vigilante jurado, y al final siempre ha sido, el trabajo se ha desarrollado en muchos sitios, he estado prestando servicios en diferentes sitios he estado de escolta, de plantón, he estado haciendo rallyes. En fin, la verdad es que tocado muchas cosas…

En el mundo del centro comercial me iniciaba en el año noventa y cinco cuando empecé a trabajar en glorias. Ahí fue cuando hubo un poco el despertar de la especialización en el mundo de los centros comerciales y desde entonces aquí sigo prestando mis servicios.

¿Qué valor añadido te ha aportado este recorrido (la visión supongo)

Sí, mi valor añadido es sobre todo que yo conozco el desarrollo de la profesión no nací siendo el jefe, Yo he mamado la profesión desde el punto más bajo lo cual te da un aspecto en el que te ayuda a entender ciertos factores que luego aprendes a ver las plantillas. Dicho con otras palabras, a mí muchas películas no me pueden contar porque yo esa película ya la he vivido. Sí que es fundamental, sobre todo el tema de la formación porque realmente empezar desde abajo y llegar hasta donde estoy … han sido muchos años de trabajo y muchos años de sacrificio si al final no te formas de acuerdo con los tiempos que van corriendo te quedas en el camino

2.- Eres el DS del Centro Comercial de Diagonal Mar. Dejando aparte las otras atribuciones que tienes, me gustaría que te centraras en el Centro Comercial. ¿Cuál es tu día a día en el centro comercial?

Pues depende de muchos factores: depende de las actividades que tenga el centro en ese día, con lo que hacerte una agenda de lo que vas a hacer cada día en este sector es muy complicado porque siempre tienes algo que altera, o pasa algo o tienes alguna visita o alguna entrevista o tienes que atender a la policía, con lo cual se altera un poco el día a día.

Pero para resumir un poco llego por la mañana me leo los informes de seguridad y los incidentes del día anterior, reviso todas las imágenes de todas las intervenciones que habido al día anterior. Para ver lo que se ha hecho, qué es lo que se ha pasado, y luego resolviendo las incidencias que se plantean a lo largo del día y pasar las novedades que pertoquen y estar en contacto con el resto de equipo de gerencia y participando en desarrollo del resto de actividades de marketing, lo que afecta y lo que no afecta a seguridad y ahora que estamos en obras pues imagínate lo que tenemos aquí. ahora es todo totalmente impredecible.

¿Cuáles son las amenazas recurrentes a las que tienes que hacer frente y qué medidas utilizas para tal efecto?

Bueno, la amenaza que más afecta al centro comercial la que más se produce, es sobre todo el hurto tanto sea leve o grave, es lo que más problemas nos ocasiona y últimamente el tema de las carteras. Los carteristas que se hacen las carteras y también los móviles. Cuando te entran al centro dos o tres personas de estas cinco o seis teléfonos o carteras caen seguro. Esto es el

día a día. Luego en cuestión de lo que pensamos que más puede ser es el tema del terrorismo. Tenemos una obsesión para poder prevenir cualquier incidente terrorista, estar encima de todo, analizamos la gente que viene, analizamos el comportamiento de la gente para detectar posibles riesgos, gente que toma notas, gente que hace fotografías, se analiza todo incluso se habla con la gente se dice y se pide que no que no haga fotos, se le mira el teléfono con las fotos que han realizado. Al final esto es una propiedad privada y tiene una normativa de seguridad que hay que obedecer.

3.- ¿Está la Ciberseguridad Integrada en la estructura de tu departamento o por el contrario se lleva desde el departamento de Sistemas u otros?

Lo que es la ciberseguridad en sí referida a los sistemas de seguridad y redes lo lleva el propio departamento de IT. Luego está el otro concepto de ciberseguridad que es lo que nosotros los especialistas en seguridad entendemos, el análisis de las redes etcétera. Hay un montón de empresas ahora recurrentes en el mercado en vigilancia digital sí que es verdad que en los últimos años hay 200000 empresas diferentes que se dedican o se están empezando a dedicar a estos temas. Yo he hablado con unas cuantas y realmente te das cuenta de las que saben lo que están explicando, las que están aprovechando la oportunidad y no saben lo que están explicando. En temas de ciberseguridad la seguridad de las redes lo lleva nuestro departamento de informática.

Si te pregunto y, evidentemente si me puedes responder, cuáles son las acciones son las últimas acciones que ha hecho tu empresa en materia de ciberseguridad, ¿cuáles serían?

Ellos están muy encima sobre todo de problemas que vienen derivados de la apertura de correos maliciosos. Nosotros recibimos una media de 3 o 4 correos a la semana donde se nos pasa las alertas que ellos van recibiendo. Sí que es verdad que nosotros en muchos casos le enviamos las alertas antes que ellos a nosotros porque nos llegan por diferentes fuentes que quizás ellos no tengan, pero las principales amenazas giran en torno a robo de identidad robo de cuentas, etcétera

¿Tienes formación en Ciberseguridad?

No

¿Cómo suples esta carencia?

Yo la ciberseguridad referida a la seguridad de los sistemas y de las redes es una cosa que en mi empresa no lo vamos a tocar porque tenemos un departamento a especialista qué son los que se ocupan. De hecho, nuestra sede donde se reciben todo este tipo de alarmas hasta en Londres. Desde ahí se gestiona todo y no se envían todas las alertas.

Hablemos ahora de Inteligencia. ¿Qué es para ti y cuál es su valor añadido??

Es una buena pregunta esto de que es la inteligencia. Yo creo que para mí la inteligencia es una parte de lo que hacemos diariamente en este centro qué es analizar las actitudes de la gente. Al final cuando tú estás analizando la actitud de una persona sospechosa estás realizando la inteligencia, estás intentando captar ciertos detalles que no son normales para después poder aplicarles un riesgo. Ese es el principio básico de la Inteligencia. Luego la inteligencia llevada al más allá, yo te diría que mi caso, y además es una cosa la que me he formado y tengo que seguir formándome, creo que es el futuro te está profesión. La monitorización de redes, la vigilancia digital, la vigilancia de marcas, todo esto es aplicable a inteligencia. Nosotros estamos empezando a hacer estudios y contactando con diferentes empresas que se están empezando a dedicar a este tipo de actividad, empresas especializadas, porque a mí me da mucho miedo cuando entras en LinkedIn y ves que hay gente que dice que es experta en inteligencia, experta en seguridad. Hay una proliferación de este tipo de expertos que luego te pones a rascar, si ves que la palabra experto……. yo la palabra experto no me aventuraría a catalogarme como tal. Llevo muchos años dedicándome a la seguridad, pero no me considero experto porque entre otras cosas me nutro de información o de aprendizaje que me llega de otra serie de gente. Con lo cual, decir que yo soy un experto lo veo un poco aventurado. Y, últimamente, han salido ya te digo multitud y multitud de expertos.

Yo creo que la gente ha aprovechado sobre todo el tema terrorista, porque el tema terrorista va ligado a todo: están los expertos en terrorismo los expertos en yihadismo, los expertos en vigilancia digital, los expertos, los expertos,

Y la inteligencia, ¿cómo la integras?

Estamos haciendo un estudio con dos empresas especializadas en el que hay una herramienta de análisis. Sobre todo en el análisis de redes en los que hay dos aspectos diferenciados porque la herramienta se puede utilizar para dos cosas. Tienes la parte de análisis en la que se hace una

monitorización y una búsqueda de palabras por ejemplo terrorismo, amenaza, bomba y después tienes la misma herramienta que hace una monitorización de todas las redes y te hace un resumen de todo lo que se habla de un activo en general que puede ser un edificio, todo lo que se habla en referencia a cosas buenas y cosas malas. Lo que te hace estar te hace diferentes informes: unos más enfocados a los factores de marketing, en los que te analiza todos los seguidores que tienes en las diferentes redes y qué es lo que dicen estos seguidores tanto la parte positiva como la negativa, y después, sobre todo en materia de seguridad, toda la que hace referencia la búsqueda de amenazas. Al final no sólo recibir esta monitorización sino saber qué hay detrás de ella. Para hacerlo tienes que tener una empresa en condiciones que te lo haga. Al final este riesgo va a desencadenar en un plan de actuación y unas medidas determinadas, si es una información real

Tengo una teoría, y creo que una vez ya lo comentamos y es que, a través de la inteligencia, podemos obtener información que, hasta su llegada, la de la inteligencia, estaba sólo en manos de las FCSE. Se ha dado el caso en el que has recibido información mediante inteligencia mucho antes de recibirla por la vía tradicional (FCSE).

Este es el escalón insalvable que hay todavía en la cooperación público privada, porque la policía no acaba de fiarse del todo de la seguridad privada del sector de la seguridad privada. La información que transmite es un poco desvirtuada y un poco, ... bueno al final te llega la información a través del conducto que tienes establecido con ellos sea con el cuerpo que sea. pero sin formación que realmente tampoco tiene no es sensible para nosotros,

El caso concreto de Moscos d'Esquadra sí que te envían a través del programa de Cooperación son sobre todo alertas lógicas. Yo, en los últimos años recuerdo que de toda la información que ha llegado solo en dos ocasiones ha sido relevante y cuando digo los últimos años estoy hablando de unos cuantos años que tiene esta herramienta de colaboración. Al final informaciones de interés para ellos …. porque si la policía está buscando un terrorista de interés para ellos también para mí sí si entra en mi centro ...

Por eso te decía que a lo mejor se trata de una información interesada porque a lo mejor te están dando la información que a lo mejor después le puede revertir a ellos en un beneficio

Digamos que la información no es bidireccional nosotros aportamos mucha más información que ellos a nosotros. Sí que es verdad que la función de ellos deba ser así, ellos tienen un trabajo más concreto que hacer que nosotros. Pero a la hora de informar nosotros les enviamos mucha información.

Volviendo a esta casuística, el que te llegue antes la información, a lo mejor La tienen y no te la quieren dar o sencillamente no la tengan. Crees que esta casuística va a cambiar la relación, una relación que ha estado marcada por la ley del 92 que subordinaba la seguridad privada a la pública y después la nueva ley la 5/2014 que la ha suavizado de Iure, pero de facto. Al final quién tiene la información tiene el poder, mi teoría es sí desde la parte privada se recibe información privilegiada crees que esto va a determinar la relación entre la parte pública y privada.

Mira yo creo que si ellos necesitan una información muy concreta de alguien vienen y te la piden, y cuando yo necesito una información voy y se la pido sin utilizar los cauces oficiales, voy a mis contactos y mis contactos vienen a mí **cuando** estamos tratando este tipo de información. Sí que es verdad que nosotros tenemos que tener mucho cuidado con la información que recibimos porque ya te digo que la información te puede llegar por conductos oficiales o por otro tipo de conductos, pero al final tú tienes que saber si esta información que te llega es verdad o no es verdad y qué hacer con ella y aplicar inteligencia. Cuando te llega una información tienes que analizarla y tienes que saber que esa fuente es fiable porque al final la información no fiable lo que haces desprestigiar la información que estás dando. Para que te hagas una idea, cuando hubo el atentado de Barcelona yo en una hora recibí algo como 350 mensajes de WhatsApp de diferentes informaciones por diferentes cauces de estos 350 solo tenían veracidad menos de 5 el resto eran todo suposiciones y falsas alarmas. Fíjate el volumen de 350 solo 5 con información verás.

4.- ¿Cómo ha sido esta relación?, Como vaticinas que se desarrollará tal relación?

En mi Caso particular es una relación muy buena**.** Además, he tenido la suerte de trabajar con todos los cuerpos policiales y siempre hemos tenido la relación muy profesional y si he necesitado ayuda siempre me la han proporcionado y si ellos han necesitado ayuda yo se la he proporcionado. ¿Cómo va a ser en el futuro? en mi caso entiendo que después de tener la red de contactos que a lo largo de estos años hemos ido afianzando y desarrollando entiendo que va a ser buena, en el caso del resto de la seguridad privada cada uno tiene que crearse esta

relación o sus contactos con el día a día. Pero creo que va a ir a mejor, la administración está poniendo las herramientas necesarias para que la relación sea una buena relación y ahí tiene mucho que ver el nuevo reglamento qué será el que afianza todo este tipo de relaciones.

. - ¿No crees que, en un mundo capitalista, donde las nuevas tecnologías han generado una dependencia enorme, en todas las esferas y en el que (me refiero a este mundo), esta tecnología y las contramedidas para paliar las amenazas que dicha tecnología genera, está mucho más accesible, sobre todo por cuestiones de presupuesto, para la seguridad privada y no para la pública???

. - Si esto es así, no crees que ambas seguridades La pública y la privada, no van acompasadas.

Yo creo que en temas de medios técnicos nosotros vamos por delante de la seguridad pública por desgracia, porque nuestros medios económicos son muchos mayores que los de ellos es lamentable, pero es así. Lo cual también es un poco contradictorio porque sí que la tecnología va avanzando y te permite hacer muchísimas cosas, pero luego como contrapartida tienes la protección de datos que te cuarta toda esta tecnología. Al final tú puedes poner muchos medios, pero al final tienes muchas limitaciones.

. - ¿Te has planeado entonces el hecho de que la seguridad privada no dependa tanto de interior y que pase a formar parte de otro ministerio, como por ejemplo el de Economía, industria y competitividad?.

No, no tiene sentido la seguridad privada ha de ser una herramienta complementaria de la seguridad pública. Nosotros somos un complemento de la seguridad pública y así ha sido admitido por todo el mundo y la seguridad pública debe aprender aprovecharse de los medios y el conocimiento de la seguridad privada. Nosotros desde luego tenemos unas funciones muy concretas que hacer que las determinan la ley y son funciones de las cuales nos vamos a salir pero la seguridad pública sí que debe aprovecharse de esto. Tenemos muchísima información de los sitios donde prestamos servicios porque además es información que te viene dada no es que la busques, te viene dada por informaciones por gente que tienes etcétera. Entonces la seguridad pública debe aprender aprovechar este filón tan importante de información. Por ponerte un caso y hablando de tecnología ahora está muy de moda el análisis facial. A través de una cámara vas a saber reconocer o ser capaz de reconocer una persona, pero la reconoces por qué ¿en qué te basas para reconocer esta persona? hay una fuente policial que te diga mira esta es la persona que busco métela en tu base datos compáramela e identifícame a los malos?

NO. Y realmente se debería sacar partido de esto, si quieres aprovecharte de mí infraestructura y de mis medios dame información y además yo no te voy a preguntar para qué la quieres si tú me das una base datos facial de 300 personas que estás buscando por terrorismo, pederasta, tráfico de drogas lo que sea yo esta información la meteré mi sistema que está totalmente protegido y mi sistema dirá Oiga si tienes aquí a esta persona que está buscando y esto va a desencadenar en una operativa que es la que tenemos ahora. Por ejemplo, con todo el tema de los coches la identificación de los coches, salta una alarma o una ventana en el sistema diciéndote que esta persona o este coche es de interés policial y esto desencadena una Serie de acciones.

De alguna manera lo que deduzco, que para que esto sea así se debería aprovechar todo el potencial que la seguridad privada tiene. De alguna manera se tendrían que mejorar los engranajes de colaboración entre la pública y la privada, es decir la colaboración en estado puro.

Sí, la información sensible es sensible para ellos y para nosotros si ellos no tienen esta confianza con nosotros para darnos esta información sensible que ya te digo que nunca preguntamos para qué. Si nos viene Mossos o policía y nos dice que busca estas matrículas de interés nunca preguntamos para qué. Nosotros le vamos a proporcionar toda la información relacionada con esta matrícula y las imágenes que tengamos sin preguntar más, creo que falta esa dosis de confianza, porque además dependiendo del policía que venga y de la forma de actuar ves que algunos que confían más y otros te dan la información mínima para salir del paso claro y hay veces en que digo sí, sí yo te voy a dar esta información pero tengo que preguntarte con que está relacionado porque si mi servicio de seguridad tienen que hacer una intervención con por ejemplo una persona un coche que estén buscando yo tengo que saber si estas personas son peligrosas y pueden ir armadas entonces ahí sí que hacemos un poco hincapié en alguna, sobre todo lo que conlleve que nuestros equipos tengan que hacer una intervención: necesitamos saber a qué están expuestos.

6.- Volviendo a tu figura, y para abordar el modelo o figura del DS, seguramente seas una de las personas que más directores de seguridad contrates.

- ¿Qué es lo que buscas en un DS?

Se lo que no busco que ya es una buena base. Yo no busco comisarios de policía o inspectores. Nosotros buscamos un perfil totalmente diferente. Primero buscamos un perfil que nos de confianza, confianza que el trabajo que va a hacer sea un trabajo comprometido. Estamos mucho por empezar a dar oportunidades a gente joven. Sí que es verdad que en el mundo de la seguridad privada hasta hace unos años no había una carrera que te de derivar a ello. Esto ha ido cambiando, sí que es verdad que luego analizas estas carreras y ves que en algún aspecto salen algo cojos en algunas materias con lo cual cuando lo sueltas en el mundo laboral esas carencias te pueden pasar factura, debes invertir más tiempo en formación etcétera. Lo que yo busco, las últimas personas que hemos contratado, es experiencia y un perfil muy determinado dependiendo del puesto que vaya a ocupar. Me refiero al sector y a la figura en concreto. Si contratamos un director de seguridad para un edificio de oficinas muy emblemático y qué son muy renombrados y que necesitan una especial atención en este caso hemos buscado un perfil de una persona con mucha experiencia en el mundo de la seguridad y con mucha experiencia en el mundo de análisis y monitorización de redes. Sí quiero un director de seguridad para que el departamento se vea enriquecido pues lógicamente buscaremos un director de seguridad, pero si tiene algún valor añadido más pues mucho mejor. Pongamos el director de seguridad que aparte de ser director de seguridad es licenciado en Derecho o abogado y que tiene o ha ejercido defendiendo a un policía a un vigilante temas de aspectos laborales etcétera. Esto lo que hace es enriquecer el departamento. Buscamos siempre una pieza que no que sea subordinada, sino que al final pueda añadir valor al conjunto. Esto normalmente, aunque no lo creas puede ser lo contrario. Yo como director de Seguridad Corporativa sí contrato a alguien que sepa más que yo mi riesgo es que me es que me quite el trabajo esto nuestro sector será mucho yo es todo lo contrario yo quiero contratar a alguien que sepa más que yo para que me enriquezca mí y a mi compañía

- ¿Cuál debe ser su integración con la empresa, con el resto de departamentos?

La integración en nuestro sector sobre todo tiene que ser total. Nosotros en las reuniones qué hacemos tanto locales como nacionales todo el mundo habla mucho de marketing, del departamento técnico, que si esto no está bien mantenido la gente no viene, si no se hacen campañas de marketing la gente no se atrae, y si no hay unos buenos locales la gente no se siente atraída pero yo siempre digo lo mismo el trabajo de todos ellos, si yo no hago el mío

bien, no sirve para nada, porque si el centro no es seguro no sirve de nada tener buenos locales buenas campañas de marketing. Al final la seguridad es un concepto y una sensación que tiene la gente. Si tú vas a un sitio y te sientes inseguro no volverás. Esto también está cambiando con el tiempo y por desgracia el asunto del terrorismo ha tenido mucho que ver. Porque sí que la sensibilidad de las compañías ha cambiado debido a esto

- **Cómo crees que va a ser el DS del futuro? (Apuntar a un perfil mucho más técnico, temas de Ciber e Inteligencia)**

Esta pregunta quizás te la deberías hacer a ti mismo porque tú estás haciendo 4 años de carrera para poder prepararte. Yo he tenido la carrera universitaria de la vida y de la formación y el conocimiento que he adquirido durante todos estos años. Esta pregunta la deberías hacer vosotros, ya que sois el futuro de todos esto. Yo te diría que sí y además te diría que con el tiempo los departamentos de seguridad dejarán de llamarse así. Yo creo que con el tiempo debería derivarse en el departamento de riesgos con todo lo que esto conlleva, un departamento que tendría que llevar la seguridad física, la seguridad humana, tendría que ir el análisis de riesgo laboral, de seguros, e inteligencia, y ciberseguridad con lo cual hace falta gente muy formada, ¿formada en todo? No, yo creo que hay que buscar especialistas no una persona que sea experta en todo, que tenga unos conocimientos de todas las materias pero que se para nutrirse de diferentes especialistas

7.- Un tema que también hemos comentado con anterioridad, hace referencia a una realidad en los puestos de DS de España, que pasa por la capitalización, en gran medida de los puestos de DS por parte de miembros de las FCSE.

Por qué crees que pasa??

Por desconocimiento de la gente que contrata a este tipo de personas. Al final hay muchos cargos son contratados por los contactos que tiene esta persona. yo te diría que con mi experiencia personal cuando yo he llamado alguna puerta siempre me han atendido sin problema ninguno, y en todas me han facilitado la colaboración que necesitaba, sin tener la necesidad de tener grandes contactos y cuando me han hecho falta los he buscado. ¿por qué se opta a ese tipo de puestos? por desconocimiento de la figura del director de seguridad. Yo creo que la policía tiene una buena formación policial pero no es lo mismo tener una buena formación policial que tener una buena formación en seguridad privada. De hecho, si te fijas en

los grandes fichajes que ha habido muchas empresas, al final contratan un director de Seguridad de estas características el comisario de no sé qué el intendente de no sé cuánto y después debajo de esta persona hay contratado un Departamento de Seguridad por los directores de seguridad para cubrir las carencias.**Yo creo que al final lo que pasa es que hay un desconocimiento no solo de la gente que contrata sino también en la sociedad de lo que es la seguridad privada, que se acentúa en los responsables de contratación, entiendo que buscan este valor añadido es que a los contactos y seguramente cuando yo les pregunte a ellos me lo van a negar, y dirán que no …, y por otro lado tú me estás diciendo que tú no has tenido para tejer estos contactos, con lo cual el supuesto valor añadido se disipa.**

Para mí sí, Sí que es verdad que en algunas ocasiones cuando se hacen este tipo de fichajes son empresas muy concretas, y sobre todo lo atribuyó al desconocimiento de esta empresa, primero de lo que buscan, segundo de perfil necesario, y tercero en la elección de la persona. Tú cuando contratas un director de Seguridad tienes que buscar una especialista seguridad. ¿Sabe más uno que ha sido policía aquí uno que no lo ha sido? habrá que ver para que lo queremos contratar.

8.- Juanjo, ¿cuál son básicamente las funciones del DS? (No quiero que me reproduzcas la ley, háblame de tu experiencia)

Las funciones son muy claras, Tú tienes que ser una persona capaz de analizar todos los riesgos que se puedan producir en todos los en tu puesto de trabajo e ir un paso por delante de estos posibles riesgos, saber gestionar y cuando digo gestionar no digo dirigir, yo no dirijo mis equipos, yo los gestiono. Tienes que ser una persona totalmente accesible para el resto de departamentos. Normalmente los de seguridad, los del departamento de seguridad son los bichos raros de la compañía solamente es vista como esta figura negra y oscura que siempre está ahí….

Hay que buscar la normalidad, un director de seguridad tiene que ser muy normal, muy accesible, que tenga empatía con el resto departamentos y que se para analizar.

No crees que te olvidas el fomentar la cultura de seguridad en todos os miembros de la empresa.

Bueno lo que pasa es que la cultura de seguridad …, hay lastres que nosotros no nos vamos a quitar de encima: Que es la exageración. Nosotros siempre llevamos estos aspectos de seguridad a la máxima exageración, y al final, lo hacemos porque el riesgo en algunos casos determina que tiene que ser así, aunque probablemente la amenaza luego será menor y tú las medidas que tomes sean menores. Pero eso pasa en la vida laboral y en casa. Yo en mi casa con mis hijos les digo no vayáis aquí porque os puede pasar esto y siempre me dicen que soy un exagerado. pero, ¿puede pasar? pues ….

Yo creo que la gente que nos dedicamos a la seguridad tenemos una especie de sexto sentido. El saber hacer entender esto a determinadas personas es especialmente complicado. Nuestro centro comercial a nivel de gerencia cuando todo el personal cuando cualquier cosa que vayan a hacer y repercute la seguridad siempre van a preguntarnos a nosotros, ¿cómo lo planteamos, ¿cómo lo hacemos? etcétera. O incluso ellos han propuesto hacer algo y nosotros hemos analizado los días y al final no se ha hecho. Con lo cual hay una buena integración y una buena cultura de seguridad. Esto en lo que respecta al aspecto local de nuestro centro. En relación a mi compañía al final de nosotros se acuerdan cuando pasa algo, porque tú puedes enviar en una semana 25 correos de propuestas de medidas y la mitad de ellos no son contestados. Ahora en cuanto hay un altercado tu teléfono empieza a sonar iba desde el jefe inmediato hasta el director general de la compañía y pregunta qué hacemos, cómo vamos a comunicar cómo vamos a tranquilizar a los clientes, qué medidas vamos a tomar. Y a veces me entran ganas de contestarle en estos 25 correos que te he enviado la semana pasada tiene la respuesta a todas las preguntas.

11.5 Entrevista Jesús Alcantarilla

FICHA TÉCNICA	
Descripción	Entrevista a Jesús Alcantarilla, Director de seguridad Monasterio de Montserrat.
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector
Fecha	14 de -marzo del 2018
Lugar	Monasterio Montserrat (Dept. Seguretat)
Observaciones	

1.- Jesús, no nos conocemos … la primera pregunta me lleva a saber más de ti. ¿Cuál ha sido tu trayectoria profesional hasta llegar a estar donde estás..?

Bueno yo vengo de una familia militar. Mi padre era militar y el concepto de la seguridad de mi casa era permanente desde bien pequeñito. Mis abuelos lo eran, mi padre proviene del Ejército, somos dos hermanos, nos llevamos 2 años, mi hermano con 16 años decide irse a la academia de Suboficiales de Lérida aquí en Cataluña. Yo siempre he sido una persona muy inquieta que siempre me ha gustado mucho el concepto de la vida, el concepto de la palabra y da la casualidad que la vida militar me gusta pero no era lo mío. A mí esto de estar en un cuartel cerrado jerarquizado, a la orden, a la orden... Aparte de la orden la disciplina es buena pero siempre tiene que haber atributos. Saber obedecer es bueno pero ser buena persona también. Yo me di cuenta de que mi padre era un buen profesional porque era buena persona. Lo primero que te voy a decir es que para ser buen profesional hay que ser buena persona, No Todos los profesionales son buenas personas pero para ser un buen profesional hay que ser buena persona. Esto me gustaría que lo dejaras claro.

Porque esto es importante para entender el concepto de seguridad. Yo conocí los parámetros de la protección prevención y salvaguarda. De pequeñito preguntaba por las cosas y me dice mi padre que habían dos entes muy importantes que eran las personas y los bienes. Las personas y el patrimonio. Por eso yo cuando tenía 14 años le pregunté a mi padre que qué era patrimonio. Él me dio una definición muy buena, y yo tengo el Máster de patrimonio, puedo decir que

patrimonio viene de la palabra Patri padre y monio recibido (lo recibido por nuestros ancestres). Esto que tú estás haciendo hoy conmigo hoy es patrimonio, una buena paralabra, eso es arte y por esto es importante que nos conozcamos mucho. Por eso para conocernos nos tenemos que conocer con la cabeza y con el corazón no con el ombligo porque el ombligo es personal y lo que hay que buscar es colectivo. Yo puedo tener un pensamiento mío de mi ombligo, pero en seguridad tenemos que tener muchos ombligos, y qué pasa, que el buen profesional es el buen bombero pero que va apagando fuegos constantemente, minimizando los riesgos, las amenazas y las vulnerabilidades, y después hablaremos de estas palabras tan importante de que todo el mundo habla y nadie sabe lo que es en este sentido. Por esto yo conocí el preámbulo de lo que mi padre me enseñaba y me enseñaba a ser buena persona y buen chico dentro de un mundo militar.

Te voy a contar una pequeña anécdota que te quiero contar porque te vas a dar cuenta de lo que es la vida en sí de mi vida profesional. Yo era pequeñito y siempre he tenido la ilusión del del auxilio de ayudar a la gente con esto con 14 años me hice árbitro de fútbol. Yo quería... yo me hice árbitro de benjamines alevines etcétera. Quería conocer el respeto pero desde dentro, no porque tengo silbato y que diga por mí se hace esto porque yo lo digo porque yo lo quiero así no se consigue las cosas. Las cosas se consiguen sumando y las sumas multiplican. Entonces me di cuenta que siendo buena persona se pueden conseguir muchas cosas, y, cuando a las personas se dice las cosas con una sonrisa con un buen gesto y con un comportamiento no verbal, lo que se llama hoy en día en seguridad sinergología, lo que tú estás diciendo sin decir nada.. Eso me di cuenta que lo mío era el auxilio, ayudar a la gente pero siempre con la palabra. Me hice árbitro de fútbol cuando tenía 13 14 15 años, terminé el bachiller y me dijo mi padre: has sacado el bachiller y tienes que hacer la mili o a la universidad. Yo era muy de seguridad del concepto militar pero yo no quería entrar en la Academia militar. Entonces le dije a mi padre que quería ser Guardia Civil. Y, ¿porque fue lo de la Guardia Civil? un día iba con mi padre ,yo iba yo tenía 16 años y me dijo que teníamos que ir a ver a un amigo suyo o un coronel, para hablarme la mili. Pues cuando terminamos de la reunión con él, al acompañar a mi padre, pasó por delante de una estación de trenes de Sevilla una pareja de la Guardia Civil. Claro mi padre era militar entonces y la pareja de Guardia Civil se cuadró y lo saludó. Mi padre le respondió el saludo y yo me quedé bloqueado, sólo por ver dos personas con un informe con una rigidez, con una profesionalidad innata una disciplina, te puedo decir hasta el tiempo que estuvo

saludando sí cuándo dejó de saludar. Cuando recorrimos 200 metros me dijo mi padre, ... pregunta no pudo haber venido major..., ¿ya sabes lo que quieres ser? y le dije sí, quiero ser guardia civil.

¿Cómo reaccionó él?

Pero eres tonto no conoces nada, es una profesión muy sacrificada y tal… porque no te vas al Academia de Militar de Zaragoza y con 22 años sales de teniente. Yo le dije que yo que quería ir al Academia de Guardia Civil, y después ascender, saber lo que es un guardia, saber lo que siente un guardia saber lo que siento un cabo saber lo que siente un cabo primero, saber lo que siente un sargento y poco a poco ir subiendo. Porque si sé lo que sabe un guardia y lo que siente un guardia cuando sea teniente lo tendré mucho más fácil.

Y esos son los conceptos, los pilares básicos, en esa triada de que para mí de pequeñito mis padres me decían que la seguridad eran los valores de lo que representa la seguridad quién protege la seguridad , y las amenazas de la seguridad. Por eso mi triada valor, protector y amenazas van con una triada muy importante que son las contramedidas de la Seguridad que se representan con la letra D : Detectar, disuadir, dilación, defensa. Resumiendo, al principio saber qué hago en base a lo que yo siento a lo que yo quiero es lo que realmente me va a hacer feliz en mi trayectoria de vida.

LLEGAS A LA GUARDIA CIVIL Y……

Llego a la Guardia Civil y entro en un concepto de lo que creo que para mí es principal para todos los cuerpos policiales he hoy en día. Y esto por favor me gustaría que quedara muy claro. Yo cuando tú me llamas, yo también hago mi trabajo y mi trabajo en seguridad, para mí la seguridad es mentalidad más actitud, un valor constante y un valor fijo. Ese valor fijo aquí entra lo que yo quiero ser, todo el mundo necesita que alguien le diga que lo ha hecho bien. Reconocer a un buen profesional por un concepto de día a día, por esto es muy importante que tú te dediques a lo que te quieres dedicar. Yo he terminado un curso formativo del personal de seguridad privada de Prosegur dedicado a Montserrat. Para mí de Montserrat hay cosas a nivel de seguridad muy importantes que tú no lo sabrás como vigilante. Ahí estoy yo para enseñarte lo importante: la historia de la palabra Montserrat. Los que nos dedicamos a este trabajo tenemos que estar orgullosos de saber lo que hemos decidido ser. Yo quiero

convivir en un bloque, el que me de lo mismo que el del cuarto sepa que soy Guardia Civil, o MOSSO. Yo tengo que estar súper contento de ser policía, no porque este señor piense o no piense. Porque mi trabajo es lo mas de uno de los trabajos que hay. Por esto el concepto de la vocación de servicio es tan importante. También te digo que esta vocación de servicio tiene que estar equilibrada con un buen sueldo. Un sueldo que te deje pensar solamente en seguridad, que no te deje pensar en la hipoteca del piso y en los problemas que tienes. nosotros estamos cada día ayudando a la gente en muchos ámbitos a nivel integral, esto tiene una recompensa, y no porque sea Guardia Civil, la Guardia Civil como los Mossos tiene una trayectoria de muchos años. Garbanzos negros los habrá en todos los sitios pero hay más garbanzos blancos que negros. lo que pasa que alomejor sólo se ven los negros. aunque a veces lo que te anima a seguir , a pesar de todos os palos en las ruedas es esta vocación.

Yo yo entro a la Guardia Civil con 17 años y lo primero que hago es hacerme una prueba y pienso ¿realmente quier ser Guardia Civil?. Yo personalmente ya en el año 82 me hago un DAFO, eso que los americanos llaman FODA. Yo me hago un Scandisk interno, Y digo ¿por qué quiero ser Guardia civil? te lo voy a decir…. Lo que me gustaba de guardia civil era el concepto de disciplina, pero quiero que quede muy claro que lo típico de por mis c****** no me gusta, me gusta que se entiendan las cosas. Un buen mando debe saber explicarse ser coherente y sensato y ganarse a su equipo. Lo que vale son los equipos de trabajo. Un líder se hace, pero líder puede ser tú o yo o todo el equipo. Aparte de líder hay una persona que se llama el referente, (quédate con esto). Los referentes son aquellas personas que son necesarias, que tienen una oratoria, una profesionalidad, una entrada, una salida, un silencio, una coherencia, una sensatez. Son de estas personas que dices " Este tío es un referente". Líder hay muchos. Líderes no deberían ser los jefes deberían, los líderes deberían ser los equipos. Si un equipo es líder todo funciona de maravilla. El patrón de un barco tiene un carnet para gobernar el barco. Lo que vale son los Marineros, tienen que tener su personalidad,su hoja de ruta, … Si a un marinero le da por remar un poquito más, el gobierno del barco no va. En este sentido toma importancia lo de ser buena persona. Cuando tú eres buena persona todo fluye.

LLEGAS A LA GUARDIA CIVIL

Llego a laGC y me destinan a Catalunya. Déjame que te cuente esto porque te va a gustar. Estoy en la GC y saco un número bueno y me puedo ir a donde todo el mundo quiere ir, pero me hago muy amigo de un catalán "EL POLACO". Amigo catalán que está aparcado, lo conozco era una persona inteligente, coherente y sensata generosa todo. Es una actitud que hoy en día se busca y me hago amigo de él. Él no es muy buen estudiante. Yo le digo, ¿tu padre dónde està? dice mira mi padre está destinado en Sant Celoni, es un sitio maravilloso en Cataluña, en la montaña. Yo lo escuchaba y me enamoro .. él me dice qué Sant Celoni pertenece a la comandancia de Manresa. Cuando terminamos más o menos la Academia saqué un buen número y el general me dice Alcantarilla tienes ahí casi todo para elegir. En la comandancia de Manresa había 225 plazas.

¿MANRESA? me dice; ¿te has equivocado?. Pero Alcantarilla como Usted, … General que me quiero Ir a Manresa qué quiere que le diga. Estaba en el sur y quiero ir al norte. Y, ¿por qué Manresa? Ta a gustar lo que te voy a decir. Cuándo se lo dije a mi familia no lo entendían. Tampoco entendieron que me metiera en la Guardia Civil y mi madre me dijo ya sé por qué lo has elegido hijo, porque Cataluña hay uno de los monasterios benedictinos más importantes que están en Montserrat. Tú quieres estar cerca de la Mare de Déu de Montserrat, y digo, yo había pensado, sí madre sí.

Yo vine en el 1982, si te acuerdas este año hubo dos acontecimientos importantes en España. el Mundial de Fútbol y otro fue la visita del Papa Juan Pablo Segundo a Montserrat. Me destinaron a Manresa, me Fui a Sant Celoni y estando en Sant Celoni llegaron dos telefonemas pidiendo voluntarios para la selección de Brasil o para la Abadía de Montserrat. Yo escogí Montserrat y el Sargento me dijo: pero usted está seguro? Usted no sabe dónde va. Yo le dije sargento me quiero ir a Montserrat yo soy de ideas fijas. Y fue lo mejor que hice. vine a Montserrat me enamoré de la montaña del factor estructural de la energía, el país en sí, de la coherencia, de la sensatez, de una buena palabra, de las personas a las que les gusta conocer, algo culto . Aquí hay mucha vida, hay mucho patrimonio, mucha historia. Aquí hay uno de las mejores Bibliotecas que hay a nivel mundial. Me vine a Montserrat y estuve 3 meses. Fíjate tú quién me iba a decir a mí que después iba a estar yo aquí de director de seguridad. Y se me cayó una lágrima y yo no soy de lágrimas porque después hablaremos de cuando estuve en la guerra, conociendo el concepto de seguridad. En el año 2007, el 17 de septiembre, después te explicaré detenidamente cómo se creó el departamento de seguridad, el Pare Prior me dice que me deja

de director de seguridad aquí y le dije si me podía ir al antiguo cuartel de la Guardia Civil, que había, que estaba en desuso porque me acordaba de esos momentos, De esa triada de sentimientos emociones y percepciones que cada persona tiene que tener consigo mismo. Yo soy muy de glamour, necesito cada día algo interesante en la vida para que me dé……. yo cuando escucho a la gente hablar con la boca del Big Data de la seguridad artificial, después hablaremos un poquito de la ciberseguridad. Hablamos de nombres pero de lo que estamos hablando….

Ya te digo, me dio la oportunidad de estar aquí. Sant Celoni, lo que es el entorno de Montserrat y después continúe mi vida en la Guardia Civil. Yo era joven y quería conocer mundo, me fui a Tenerife donde me mandaron al Hierro. Estuve muy bien allí, aunque me asfixiaba porque era una isla muy pequeña y yo necesitaba más. Me fui a hacer el curso de formación de policía judicial, de tráfico donde estuve muchos años. Después de Canarias me fui a Madrid y después de Madrid a Barcelona. En Barcelona estuve muchos años en el subsector de atestados de Barcelona donde estuve muchos años. Y acabé harto de muertos. Con 22 añitos pensé que sí sí pero necesitaba algo más, estaba cansado de tanta investigación y tantas tantos accidentes. Y un buen amigo mío que a lo mejor lo conoces, Jaime La barca, era catalán había sido guardia urbano se fue a la academia de la Guardia Civil que era un catalán catalán bueno y pidió tráfico y nos tocó juntos en Navas de Tolosa. Un día estando juntos me dice: tú tienes el perfil para irte la Casa Real. yo le dije: ¿yo a la Casa Real? yo con tal de salir de atestados lo que fuese pensé, estaba saturado de tantos accidentes y de tantos accidentes, diligencias y tal. Y un día como Murphy no descansa nunca llegó un telegrama pidiendo personas para la casa real con un perfil determinado. Yo me acuerdo que otro compañero y me dice mira lo que ha llegado esto es para ti, y yo le dije: tonto estos para hacer garita en el Pardo. Digo mira si me meten a mí una garita digo déjate.

ESTABAMOS …..

Al final mando la solicitud, pasaron un mes y dos meses y no dijeron nada, Un día tomando el café con él me dice: ¿de aquello que? y yo le dije nada de aquello nada. A las 2 horas bien el capitán con un telegrama diciendo señor Alcantarilla ha sido usted seleccionado para la prueba de la Casa Real, pensé para mí el puñetero Murphy que no descansa. Me fui a Madrid y hay cambio mi vida. Yo soy una persona que necesito estar en un sitio que yo pueda dar algo.

Cuando tú me…. y cómo va a haber un proceso de amistad y nos vamos a conocer y ya haré yo para estar junto contigo, cuando tú me veas que yo no tengo la sonrisa en la cara piensa algo le pasa a Jesús. Yo, no quiero estar en un sitio que no esté agusto nunca. Yo estoy en los sitios para ayudar, y ser un buen soldado. Tengo un problema que no puedo ni tolero las injusticias **En este aspecto nos parecemos bastante,.. A nivel profesional me ahoga también el no poder crear, de hecho he dejado buenos trabajos por no poder aportar más. Siempre lo que me ha hecho estar en los sitios es poder ofrecer algo.**

Déjame que te haga una apreciación en el concepto de la seguridad que tú bien sabrás como buen profesional que eres. Todo que se hable aquí lo puedes comprobar si buscas en Internet en todo lo que hago lo que escribo los artículos…. lo bonito es mirarte a la cara,.... ¿que fallo? cómo ser humano seguro que sí aunque intento no hacerlo pero seguro que sí. Yo puedo equivocarme. Cuando te cuente lo que me pasó en Bosnia te va a venir muy bien desde el punto de vista empírico de lo que es el concepto de la seguridad en sí. Yo me fui a Bosnia , Yo di todo por una medalla y me traje una separación. Hay gente que se va para ganar dinero y otros para hacer carrera yo me fui a Bosnia por saber lo que la gente padece en la guerra. Por eso me fui. Se presentaron un montón de suboficiales para ir y me escogieron a mí. Que no te engañen diciendo que van forzados. Van todos voluntarios porque hay unas compensaciones económicas muy buenas. Te pagan tres veces el sueldo mientras estés. Yo me fui por una medalla y me traje una separación ahora te lo contaré. Eso también es bonito en la vida ser sincero sincero con uno mismo y cuando uno se equivoca decir me he equivocado. Yo me he equivocado muchas veces. A veces decimos que mentimos sin darnos cuenta. Yo siempre digo que aquí puedo mentir poco porque tengo 7 confesionarios de Montserrat y los monjes me cogen la matrícula … Pero seguro que algunas mentirijillas decimos también sin darnos cuenta. Yo estoy siendo sincero contigo y no te puedo traicionar porque si te traiciono a ti, me estoy traicionando a mí. Yo quiero ser feliz conmigo para quererme a mí y así poder quererte a ti. No sé si estuviste en la última clase que yo di .

No porque siempre que ha habido alguna salida aquñi, no he podido por temas de trabajo, …

Me hubiera gustado que hubieras estado porque tu jefe de estudios que es muy pícaro se dio cuenta de algunas cosas. A mí siempre me gusta prepararme porque gente interesante que puede venir, gente muy interesante para hablar. Yo tengo facilidad con la palabra y por mi forma de ser, me entiendes, ... me gusta dentro de la obra de teatro hacer la escena que

toca. Porque la vida, quédate con esto, es una obra de teatro. Cuando estás en la guerra te das cuenta lo que es la vida, lo bonito el nacimiento de cuando sale el sol y cuando te pones a valorar lo que es una buena amistad, y cuando estás con tus compañeros uno en el norte y otro está en el sur, puedes decir aquí estamos los dos por una misión, es salvaguardarnos. Es aquí dónde viene la sana amistad que siempre viene de una palabra y de un contexto.

Yo estoy en la casa real durante unos años, aquí puedes ver algunas fotografías con el rey de cuando vino a Montserrat. Estuve muy agusto en la Casa Real lo que pasa es que hay un problema en este mundo de la seguridad, hay gente que se cree que es el rey del mambo por el simple hecho de acompañar una persona y no son nadie . Como buen profesional me vino la cabeza estudiar la morfología de lo que es un escolta un gorila y un guardaespalda. Como tuve la suerte de estar en Estados Unidos dando clases, luego también hablaremos de la época en la que estuve estudiando en Israel el Curso Superior de director de seguridad, y estudié la sinergología. Porque tú te colocas de determinada manera,... todo es por un tema interno humano fisiológico de cada uno de nosotros cuando nos reímos cuando no nos reímos lo único que no se sabe es lo que tú estás pensando internamente dentro de tu cuarto de seguridad. Yo puedo estar con una persona y me puedes decir si puede estar pensando vaya rollo de tío no veas la que me está soltando.

Estando en Casa Real viví momentos bonitos desde punto de vista de lo que supone conocer una Casa Real que es una familia real. Una familia como la tuya o como la mía: igual, que se levanta por la mañana desayuna igual que tú, se duchan y se lavan… Son personas que a nivel binomio patrimonial historia tienen una serie de ventajas que a lo mejor por su condición de ser otros no lo tenemos. Hice mi trabajo estuve con rey y reina durante mucho tiempo, conocí todo el círculo. Yo soy de conocer todos los círculos, no me gusta estar arriba si no he estado abajo. Prefiero estar en el subsuelo y mirar lo que hay en el subsuelo para poder estar arriba. Para poder determinar dónde está lo importante, la contravigilancia, de vigilar a quién te vigila, al hombre gris ese es el importante el que reconduce el que valora el que examina, el que prevé. Esto es lo importante el concepto de la seguridad. Bien, estoy en casa real, y conozco a una chica de Sant Celoni y estoy con ella que se venga a Madrid y al final me vine yo y me fui a Sant Celoni, dejé la Casa Real. Se enfadó mucho el ayudante de cámara conmigo porque yo había encendido acabo y me dejó allí….. es importante que sepas esto, a partir de teniente, en

seguridad, quién elige quién se quede es el rey, pero de guardia a Sub Oficial Mayor es el jefe de la Casa Real el que da el visto bueno.

Me vine a Gerona de Policía Judicial estuve en Gerona muchos años. Después de ascender a sargento me vine a Navas de Tolosa a tráfico.

Un día llegó un correo para seleccionar suboficiales voluntarios para la guerra. ….. yo por la noche tengo la costumbre de todos los actos que hago durante el día, 5 minutos en silencio con los ojos cerrados y pensar en las veces que metió la pata, las veces que he hecho lo que no tenía que hacer, o a quien lo has mandado a la m***** que tenías que haberlo mandado a la m***** esto también pasa.

UNA RESTUCTURACIÓN COGNITIVA, VAMOS,...

Yo soy del tipo de personas que el 99% de veces me gusta ayudar a la gente pero hay un pequeño 0,0 1% que cuando pasas la línea roja sé decir que no.

Bien, al final pedí lo de suboficial y da la casualidad lo que es la vida que en operaciones internacionales cuando pido la instancia un amigo que había estado conmigo de Coronel ascendió a general se pasó allí a operaciones internacionales de la Guardia Civil. Cuando llegó mi solicitud dijo c*** estás en Alcantarilla, y me llamó y me dijo: ¿que haces que he recibido un correo,¿ todo bien ,¿la mujer bien, la familia bien?, si tengo una niña de 4 añitos pero mira me ha entrado el gusanito y quiero conocer la vida de una guerra. -**INTERRUPCIÓN TELÉFONO-**

Me dijo piénsatelo tienes tiempo para pensártelo yo le dije no no mi general ya lo he pensado. Me llevan a Zaragoza tres meses antes y estoy allí cuatro meses. A nivel de seguridad aquello fue un antes y un después. Allí aprendí a saber escuchar a la gente, ponerte en su lugar y sufrir con ellos. Yo tuve la suerte que iba en un contingente de guardias civiles, llevaba cinco cabos y 25 guardias. Hacíamos fiscal, antidroga, tráfico, hacíamos el Convenio de Seguridad Pública en la guerra, allí estaba la OTAN y por lo tanto estaban todos los países y tráfico lo llevaba la Guardia Civil. Y ahí había unas normes, el tío que se pasaba dos veces lo metieron avión y lo devolvía a su país. Ese buen poder lo utilicé desde el punto de vista de lo que yo necesitaba en Bosnia. Me hice muy amigo del capitán de cocina, íntimo amigo, y cada día cuando terminamos de comer le decía Manolo cuantas patatillas te han sobrado? me decía hoy tengo dos cajas… oye Manolo había habría algún día algún fuet bueno algún choricito algún jamoncito??.... y le digo al cabo que se pase esta mañana con una caja y se lo metes ahí. A lo mejor se pensaría que estamos haciendo contrabando y todo. Yo me iba de asentamiento en asentamiento y le

regalamos caramelos a los niños y aunque eso era muy peligroso .... tenía que tirar los caramelos en marcha porque si paraba el coche ya no podía arrancarlo. Tuve la suerte de conocer en una casa aislada, a mí me gusta mucho el campo soy mucho de la orientación y me iba con escolta policial y di con una casita con una abuelita que tenía 83 años con su marido de 79 y con tres niñas pequeñas que la guerra habían perdido sus padres. Eso fue un antes y un después en mi vida. allí entendí lo que es el concepto de la generosidad, es la palabra más compleja del Diccionario de la Real Academia Española. Ser generoso implica muchas cosas. Yo siempre llevaba un quesito alguna cosita. Y me dijo ¿qué te doy yo Jesús? y me daba la zurrapa. El café era tan malo que nadie quería venir conmigo de lo malo, de mal que lo pasaba yo arresté un cabo por no aguantar el dolor porque aquel café era insoportable. Yo no podía vomitar porque me estaba dando lo único que tenía. Aquello era vamos que se caía los dientes, entrabas a la casa y un olor insoportable. Yo me enamoré de una niña pequeñita que estuve apunto de traerme, estuve a puntito de traermela. Entendí más el dolor, el silencio y mi trabajo. Me vine a España y seguí con la familia, A mi hija casi no la conocía fui al colegio y fue un drama cuando la vi porque en 4 meses los niños cambian mucho, ... bien fue un antes y un después. Tuve la mala suerte de que mi suegra y mi suegro murieron y yo no pude venir al entierro fue un cúmulo de circunstancias Y yo soy una persona muy práctica y muy coherente en ese sentido. Dos en casa dos no discuten si uno no quiere. Mi mujer era maravillosa. Yo siempre hablo bien de todo el mundo cuándo toca y cuando no no se habla. Llegamos a un punto que hubo como si fuera un grifo que caía una gotita de agua una gotita de agua y pensé dos personas que no están agusto deben separarse. La vida me devolvió la suerte ahora estoy con la persona desde hace 15 años. La vida también te da alegrías.

Cuando terminé de Bosnia me vine aquí y cuando vuelvo aquí a Catalunya me llaman de la Academia de Suboficiales para hacer unos cursos de especialización, y me escogen por haber estado en la escolta al Academia dónde están los carabineros, los Marichalar, y dentro de la Unión Europea hay un convenio de colaboración de las policías que pertenecen a la Unión Europea como lo es la Guardia Civil. Estaban también los gendarme, los carabineros, cada año escogieran un país, ese año fue Italia y personas de otros países van a dar clases de según qué especialidad y a mí me tocó protección de personalidades.

Otra etapa de mi vida que cambio mi vida. Conocí la hermandad, conocí el grupo. Hice un máster interno, del que lo importante es conocer a las personas y conocerte a ti y para saber

trabajar con tus defectos y virtudes porque todo el mundo tenemos defectos y virtudes. Lo que importa es que el corazón se alinee con la cabeza no que el ombligo vaya por el suelo.

Fue una etapa muy bonita y después cuando estaba un día en Navas de Tolosa, te voy a decir muchas cositas y según qué nombres no te voy a decir. Ahí venían mucho los compañeros de mossos. Yo estaba en tráfico y venía mucho Milans, el que fue jefe de los Mossos y un comisario que estaba en Manresa que tiene la carrera de etología que que fue comisario de tráfico ahora no me sale el nombre. Cogimos mucha amistad y mucha confianza. Coincidió la época de cuando los Mossos de Escuadra estaban entrando porque era el tema del despliegue. Yo tenía una gran amistad sobre todo con Milán. El amigo mío de la XXXX de Banc Sabadell y me dijo ostia tú te tienes que venir con nosotros a los Mossos d'Esquadra. Yo le dije ya me gustaría pero es que soy muy verde. Yo estaba estudiando para teniente. Mira lo que es la vida que ese mismo día me llama el teniente coronel urgente que vaya a verlo y me dice: tenemos que hablar. En el año 2000 hubo un despliegue de movilidad interna de la Guardia Urbana de Barcelona no sé si te acuerdas, **NO, NO,** yo pasé a la urbana de Barcelona, este jefe, este pasó de segundo jefe de lla Guardia Urbana. Fue cuando la banda terrorista ETA entro aquí. Al atentar la banda terrorista, el alcalde Clos, con el jefe Vidal, y me dice:¿ qué hace un agente de la Guardia Civil en la Guardia Urbana? le dije yo: esta pregunta no me la puedo hacer usted esta manera. Estoy entrando en la Guardia Urbana y aprendiendo. Dio la casualidad que crearon la unidad de escoltas, de este teniente coronel era muy amigo de un intendente de la Guardia Urbana que le preguntó que le pidió... que necesitaba gente con conocimiento de escolta y le dijo que conocía a la persona que me conocía a mí y que había estado de escolta en la Casa Real.

Pedi excedencia voluntaria en la Guardia Civil me fui a la Guardia Urbana donde estuve hasta el 2007. Dentro de la urbana estuve en el grupo de escoltas, estuve con el presidente del Partido Popular, estuve de contravigilancia con casi todos y un día como tenía el título de director y jefe de seguridad robaron un cuadro en París y el alcalde Clos va a París y la responsable de Cultura del Ayuntamiento de Barcelona le pregunta al alcalde. Oye, ¿cómo tenemos nosotros el tema de los museos?. Que no nos pase igual que aquí mira la prensa. Al día siguiente me viene el ayudante de cámara del alcalde y me dice oye Jesús tú tienes en tu currículum que eres director y jefe de seguridad no? A ti te gustaría ser director de seguridad del Museo Picasso de Barcelona? le dije yo ¿el que está en la calle Montcada? ¿no tiene director de Seguridad ese museo? Bueno bueno yo nada más te digo si te gustaría hacerlo. Hombre yo soy un amante del

patrimonio y claro que me gustaría. Entonces me puse en contacto con Esta chica. Estuve desde el año 2002 hasta el 2007 5 años en el Museo Picasso de Barcelona y un día me llega la directora es que te quiero unir cómo llego Monstserrat... llegó la directora y me dice que me están llamando el director del Museo de Montserrat que tiene problemas con los planes de autoprotección y yo le he dicho que tengo un buen director de seguridad Y tal. y yo le dije ¿dónde? me dijo en Montserrat. Montserrat allí arriba? ¿y por qué te ríes? porque lo conozco porque estuve allí de Guardia Civil. Me dijo que si sería tan amable de ir allí y yo le dije que si ella me lo decía yo iría Montserrat. Fui a Montserrat y me reuní con diversas personas y me dijeron que tenían muchos problemas de seguridad. Yo les pregunté por los problemas que tenían y básicamente era una empresa de seguridad que se estaba quedando con ellos. Yo le dije que ese problema se lo solucionaba yo en 2 minutos y medio porque el artículo tal de la ley decía…..

Dio la casualidad de que el jefe de seguridad de la empresa lo conocía yo, era un policía nacional y yo le dije, macho ¿qué estáis haciendo ahí? ¿solucionar los problemas?... Cada día me llamaban de Montserrat y la directora me decía te están llamando mucho y le dije mire usted, igual que me dijo que les atendiera si usted me dice que no lo haga no lo haré. Ella me dijo no no…. Un día me llamó el director y me dijo quiero usted quiero que usted me haga un planteamiento de la seguridad y yo le dije la seguridad se llama cultura de seguridad y tenemos que entrar en lo que es la cultura de seguridad. Yo le dije mire usted como usted es una persona muy inteligente primero vamos a hablar de la palabra cultura, ¿qué es cultura de la seguridad? y después le vamos a dar la vuelta a la palabra y vamos a poner la seguridad en la cultura. allí fue donde ya entró.

Después hablaremos del proceso de la seguridad y de algo que no le gustarà. La seguridad es un coste necesario no es un gasto es una inversión, y el 99% de la gente que no tiene cura de la seguridad sabe que la seguridad rebasa la cuenta de explotación. NOOOO!!! totalmente en desacuerdo, lo que hace la seguridad es darle mayor empuje para que todo funcione bien. ¿Usted se imagina que Monserrat no funcionase la luz? ¿cómo comen ustedes? sí aquí se vive de la restauración cafeterías etcétera... le costó una semana asimilar el concepto filosófico que yo tenía de la seguridad y me dijo tú tienes que hablar con el mayordomo. Aquí en Montserrat hay muchas Figuras. hablé con el mayordomo y me decía el mayordomo... ¿esto cuánto me va

a costar? y yo le dije no vaya usted por ahí, no sé lo que le va a costar primero tengo que venir y tenemos que entrar en lo que es la mnemotecnia en seguridad. Yo le decía mire usted, el problema mío es que yo hablo del contexto mío de seguridad. ¿Me deja qué de la misma forma que yo aprendo con usted usted aprenda conmigo ? Mira usted, la mnemotecnia es la ciencia de saber diferenciar el concepto de la Visualización, observación y visión. Son tres Conceptos que son diferentes yo ahora mismo te estoy viendo te estoy observando y visualizando Pero son tres conceptos diferentes. Yo te puedo ver, visualizar a ti pero también puedo visualitzar, observar y ver otras cosas y yo le ponía un mapa delante. Le decía esto es como el Norte Sur Este Oeste, sentido y dirección por ejemplo si yo le digo ahora que coja el coche y se vaya hacia Monistrol usted cómo va? él me dice dirección, Y yo le dije no está equivocado eso es el sentido , La dirección es derecha o izquierda.

Hay que modificar el concepto de la palabra en base a la elegancia de la palabra. Cuando el conoció el concepto que yo le presente de la seguridad le encantó. Y después lo más importante es que usted no me ha preguntado una cosa y yo le dije ¿esta visión de seguridad mía cómo encaja en la religión en la religión? Allí lo desmonté esto se llama laboratorio siglo 21 . Primero lo que tengo que saber es saber el tipo de gente que viene aquí que seguramente serán mayores de 70 años y no le puedo decir yo que por mis c****** no entra el coche lo primero que hay que hacer es ganarse a las personas y, ¿cómo se gana uno a las persones? pues con una sonrisa con una buena palabra… cuando ya el monje vio todo esto pensó: ¿este tío de dónde ha salido? Entramos en una buena dinámica y me dijo: al Prior. Yo soy el del dinero pero el Prior es el que tiene que decidir. El Prior me tuvo 2 horas solamente escuchando no dijo ni una sola palabra. ni una palabra, solamente bon día y gracias es un placer. A mí lo del Prior me mato me sacó de mi línea de confort, comprendí lo importante del silencio cuando más hablas más te equivocas. Por eso hay un refrán muy bueno en seguridad que dice que si no quieres decir una cosa no la digas. Este conocimiento me hizo cada vez subir un escalón, y cuando estuve en la primera planta me llamaron día Y me dicen, (fue el día más importante de mi vida) porque te tengo que decir una cosa. en este día me ofrecieron tres trabajos a la vez. un trabajo por ética no te puedo decir cuál es.

INTERRUPCIÓN TELF-

Estaba en una pizzería la calle montcada y me suena el teléfono. Me llamaron de Montserrat y me dijeron que iban a crear un departamento de seguridad. Él me dijo que yo le dije que les iba

a llevar en todo y yo le dije que sí. Yo no lo sabía que me iban a ofrecer un trabajo y él me dijo: ¿no està usted contento?. deberíamos hablar y yo le dije yo no lo entiendo padre, y él me dijo usted será nuestro director de seguridad ¿no? o sea que aparte de crear un departamento de seguridad usted me está ofreciendo irme a Montserrat y me dijo sí. Yo le dije: me siento muy afortunado padre pero necesito un tiempo porque primero yo nunca he pensado que iba a hacerlo y tengo una familia, una institución que quiero mucho también, que estoy muy a gusto en el Museo Picasso. Él me dijo tome usted el tiempo que necesite y me llama. Colgué y al momento me suena el teléfono otra vez. Era el director del museo y me dijo Jesús dónde estás y me dijo puedo venir a verte y le dije sí. yo le pregunté hay algún problema o algo y me dijo no es que he estado dándole dándole vueltas y yo entiendo que tú necesitas responsabilidad y quiero darte aparte de la seguridad funciones de dirección de operaciones, quiero que seas mi mano derecha, esto tendrá una recompensa económica. y el me preguntó que qué me pasaba porque se me notaba mucho… Yo le dije en primer lugar te pido disculpas porque yo lo llevaba en silencio porque era un tema de la directora antigua, el tema de Montserrat. Le dije que se iba a crear un departamento de seguridad en Montserrat y que me lo habían ofrecido. Yo le dije que en ese momento tenía que ser respetuoso conmigo mismo y me tenía que hacer mi DAFO particular. Ese día estoy en mi despacho y te voy a decir hasta dónde puedo llegar, y no te estoy mintiendo me gusta la palabra. Me llaman de la Dirección General de la Guardia Civil. Tengo al general tal que quiere hablar con usted. y yo pregunté qué cargo ocupa este general y me dijo que era un asunto de Estado Mayor. Hablé con este general que no conocía de nada y me dijo que le habían llegado informaciones mías que estaban muy contentos de la imagen que usted está dando del cuerpo. Me dijo oye mira (siempre hay una frase que está pensativa él pero él sin embargo). Me dijo oye mira que hay un señor, una institución muy conocida en Cataluña Qué necesita un XXXXXX. Yo soy amigo del director general y he pensado que tienes un perfil muy válido por esta parte. Yo le dije muchas gracias y le dije hoy mismo no sé qué está pasando y me voy a ir a comprar un décimo de lotería porque hoy me toca… Jesús tú no puedes denegar la entrevista…. yo le dije no que no iba a ir… me ofrecían el doble de lo que estaba ganando el sitio que estaba no era un problema de dinero. El dinero es importante pero no es lo más importante. Cuando uno gana suficientemente dinero para estar agusto la unidad familiar es muy importante… Ser empático con uno mismo con la familia, tener vida. La calidad de vida es muy importante en este sentido.

Al final decidí lo que mi corazón me dictó. Se lo dije a mi mujer y me dijo oye Jesús, ¿tú cuántos años llevas en el Picasso ?? Tú eres joven, dale una oportunidad. Yo le dije me voy a encontrar Montserrat como me encontré el Picaso, allí hay no había nada de nada de nada. Antes no cumplíamos nada ahora cumplimos algo. Fuimos poco a poco.

Acepto lo de Montserrat y aquí sí que te quiero decir tres cosas que me está dando Montserrat. Es muy difícil desde el punto de vista de la responsabilidad que tiene, el contexto de la montaña el número de personas que pasan por aquí, el concepto de la espiritualidad y del patrimonio.

Hay que saber cómo está Montserrat, cómo se gestiona la montaña, sus dueños, la comunidad benedictina son tan inteligentes que crearon el Departamento de Seguridad para que no lo crearan otros. ¿Que me ha dado Montserrat?

A mí Montserrat me ha dado mucha tranquilidad a nivel interno, mucha cultura, me ha gustado conocer a las personas, y saber leer, saber leer.

ME ACOMPAÑA A OTRA SALA PARA ENSEÑARME MÁS DE MONTSERRAT.

Lo primero que tengo que hacer es saber la historia de Montserrat. S estos son mis sueños yo tengo que saber cuáles son sus problemas. Tengo que conocer. El concepto de la inteligencia, aparte de la seguridad es importante la coctelera información, poder, conocimiento y saber qué es lo que genera Montserrat.

Dentro de los riesgos, todos los riesgos que hay en el mundo los tiene Montserrat. No hay un riesgo que no tenga Montserrat mira lo que te estoy diciendo. Busca un día un riesgo que no tenga Montserrat. Riesgo es la contingencia del daño. Para que haya riesgo tiene que haber una suma de vulnerabilidades y amenazas. Las amenazas son los detonantes de los riesgos potenciales, y las vulnerabilidades es la resistencia y la fragilidad de las personas ante los riesgos.

Es importante el conocimiento del director de Seguridad un director de Seguridad es un gestor que lo que hace es facilitar la toma de decisiones pero sabiendo desde el conocimiento. Y eso no lo da un título de seguridad de director de seguridad. Ahora yo lucho por vuestro grado, pero esto es lo que he visto en vuestro grado. Quizás tú no porque vienes de la seguridad pública, porque tú cultura de seguridad ya viene anteriormente porque tú has escogido ser lo que eres.

¿Te estás dando cuenta que si tú fueras el jefe de estudio, que es una excelente persona, le darías una visión, un enfoque diferente?. Esto que has hecho tú de que me llamara una señora diciendo que buscabas una persona corporativa yo ya te digo que chapó. ¿Sabes porque te digo chapó? porque esto que tú has hecho, el que tiene ilusión de hacerlo, lo tenía que haber hecho todo el mundo .

Lo que te decía que aunque estos chicos lleven 4 años estudiando no tienen el conocimiento o mejor dicho la preparación porque no tiene la experiencia para poder dirigir un departamento de seguridad. ¿Por qué se hacen las prácticas en cuarto? no digo que se hagan en primero pero sí a partir de segundo. Yo lo que no quiero que este grado de seguridad sea una fábrica de hacer chorizos de cantimpalo. Ahora salen 25 pero esto es una maquinaria que no parará. Puede pasar lo que pasó con criminología y eso no lo quiero yo quiero que la gente que la cantera salga en forma. Esta es la cultura de la seguridad y estos enfoques son importantes en el mundo del director de seguridad porque el director de seguridad lo primero que necesitas experiencia.

Yo cuando hablo, lo primero que hago es prepararme, y ahora escucha esta frase que te va a desmontar : Ni puñetera idea de seguridad . porque la formación es un aprendizaje continuo.

Cuándo a mi Ana Aisha me dijo si yo podía tal…… le dije exponme, no me digas solamente que quiere ese compañero de mí. Ella me dijo este compañero lo que quieres esto esto y esto. Y yo le dije ya le puedes felicitar porque ya he tenido la capacidad de pensar y esto es lo importante saber hacer las cosas.

INTERRUPCIÓN

Ahora vamos a hablar de la persona……

2. Los puestos de directores de seguridad, en la mayoría de los casos son ocupados por los ex miembros de las Fuerzas y Cuerpos de Seguridad. Yo vengo de dónde vengo, y el conocimiento que me da el grado en materia de seguridad me hace replantear, que como yo concibo de la seguridad, con la responsabilidad que requiere un puesto director de Seguridad me pregunto si solo con ser un ex miembro de los Fuerzas y Cuerpos de Seguridad es suficiente y en todo caso ¿cuál es su valor añadido y porque están ocupados los puestos por ex miembros de las Fuerzas y Cuerpos del Estado?

¿Te digo lo que quiero decirte o lo que siento???

Esto, qué tiene que ver ser teniente de la Guardia Civil o comisario de los Mossos de Escuadra con llevar un departamento corporativo??. un departamento corporativo es integral se tocan todas las PAUTAS de la seguridad. Hay un concepto de la seguridad que es la estrategia y la táctica. A mí como Guardia Civil, yo tengo una cultura dentro de la Guardia Civil y me han enseñado ser un guardia civil pero no me han enseñado a hacer un análisis de riesgo ni un plan de seguridad, ni una coherencia sensata el día a día de lo que es Montserrat. ¿Qué tiene qué ver un teniente coronel con un departamento de la Seguridad? No tiene que que ver nada. aquí entramos en el concepto de Seguridad Pública y de seguridad privada.

La seguridad privada nunca debería haber existido, porque la pública es la que tiene la competencia de llevarlo todo ¿que pasa? que como la seguridad pública no tienen ni los recursos ni las arterias para poder llevarlo, se acaba contratando, y comprando. El problema no es ese el problema es que el país tiene que dar recursos a todo. Si no hay Mossos tendré que hacer más promociones. Después lo que ha pasado es que se ha capitalizado desde un punto de vista del negocio de la seguridad. Ha habido líneas de negocio por las empresas de seguridad que están aportando mucho para la seguridad, al Estado y están generando un segmento. ¿qué pasa con esto? que todo tiene que tener una legislación, dónde la seguridad pública se complementa y se coordina con la privada.

Sacan la figura de la seguridad. yo voy a Madrid Para sacarme el título de Director de Seguridad. Yo no voy a criticar nada porque yo construyo. Yo creo que se puede hacer todo. Un director de seguridad debe ser un licenciado, un graduado en seguridad le guste a quién le guste porque yo como director de Seguridad ocupo un cargo directivo. Si usted no quiere seguridad tendrá otra cosa...

La Seguridad no la hace solo un departamento, la hacemos todos, , …. quédate con esta frase. Desde mi director general, Porque tiene que tener una cultura de seguridad, por esto yo me tengo que formar para poder administrar todo esto. Desde el punto de vista profesional no tiene nada que ver. Ahora bien este comisario estudia para la seguridad y cumple con los valores y con los criterios necesarios se puede presentar como cualquier persona pero no por el hecho de ser un coronel de la Guardia Civil o intendente de los Mossos d'Esquadra y por ello quitarle el puesto a otro.

3**.- En un mundo en el que la empresa privada tiene más recursos, recursos que le ayudan a obtener información de primera mano que la parte pública no tiene, me refiero bàsicament a la inteligencia, crees que esté privilegio de obtner la información de primera mano, va a cambiar la relación ente la Seguridad pública y la privada, teniendo en cuenta que quien tiene la relación tiene el poder?**

Eso debería ser como tú dices, …….

Lo primero tenemos que separar lo que es una ley y un reglamento. La ley reina y el reglamento gobierna. Estamos en una dinámica, en el que la seguridad privada en Europa ha habido un antes y un después y también en España. España está muy bien valorada en cuanto a seguridad pública tenemos unos cuerpos policiales maravillosos. Entramos en el concepto de fuerzas y cuerpos de seguridad, dejamos el Estado aparte. Al final hablamos de toda la policía que trabajamos policía autonómica Policía Local, Guardia Civil y Policía Nacional. Tenemos la ley 23/92 que efectivamente hablaba de subordinación. Piensa que antes el vigilante de seguridad cuando era guarda jurado agente de la autoridad en el cumplimiento de sus obligaciones.

Ahora esto no es así, hasta que el Ministerio del Interior no confíe en el personal de seguridad privada …… Usted me tiene que dar a mi confianza. Y la confianza se basa en que yo tengo que desempeñar una función….. después llega la 5/2014 y a mí que me gusta entender y leer digo coño yo le puedo sacar a esto muchas cosas. ¿Sabes lo que le sacado ya está Ley? te voy a ser muy claro: yo de dinero tengo poquísimo más bien más bien nada pero tengo recursos, y tengo experiencia y aquí es donde está lo bueno de un director de seguridad que no es dinero es capacidad de la persona. Y aquí es donde está la pregunta que tú me has hecho, yo me voy a la 5/2014 y me dice dos cosas la complementariedad. Y digo coño en el 2009 me coge mi comisario Roma que estaba en la región central y me dice qué te parece a ti ... yo no entiendo Montserrat sin Mossos d'Esquadra….. Si una persona viene aquí XXXX después de un riesgo antropico un robo o hurto lo que sea no es normal que tenga que ir a Manresa a poner la denuncia. Eso no es seguridad eso es inseguridad, tenemos que facilitar que venga la gente. Y aparte quiero que la policía de mi país se vea. Si voy al aeropuerto y veo un mosso aquí debe ser lo mismo. Me dijo es una idea muy buena y trabajamos en esto. Y es que en la ley 5/2014 me dice que cuando yo trabajo con la seguridad pública mi personal son agentes de autoridad, ojo a las órdenes de la seguridad pública.

Al final hablé con uno hablo con otro y entramos en una dinámica.. y llega un comisario, me ve y me dice adelante ,... me voy a la comunidad, lo explico... Y me dice, ¿a ti te interesa la seguridad pública aquí?, y yo le dije claro que me interesa. Porque cada día la vida es un teatro yo hago mi escena dentro del teatro, yo soy el director de Seguridad y sé cuáles son mis funciones.

Al final lo que a mí me interesa es Seguridad en Montserrat. Es poder hacer un plan estratégico y poner a trabajar la seguridad pública con la seguridad privada. Es lo que se denomina según la ley, la seguridad compartidada. Con con este modelo con el que trabaja Montserrat no hay ninguno.

Aquí hay que conocer el terreno. No hay ningún Mosso que esté y no quiera estar yo hago todo lo que puedo por cuidarlos.

Yo entiendo la filosofía de la cultura de seguridad y lo comparto por eso tenemos un convenio de colaboración como modelo propio de Montserrat.

Cada año ponemos en común la memoria de seguridad con los cursillos con los comisarios de la región y Jesús alcantarilla. Gracias la marca Montserrat, a la imagen de Montserrat, potencia en el departamento de seguridad.

Tengo que hacer una actualización que me dijo tu jefe de estudios, cuando yo hice una ponencia para tus compañeros y yo hablé de geopolitica y yo me dí cuenta que pasó algo raro porque los comportamientos no verbales los capto al momento , …. Nadie me ha dicho que el jefe de estudios era profesor de geopolitica.

Cuando terminamos me dijo tu jefe de estudios, ¿Tienes 2 minutos? Me quiso decir que en un profesor, los tiempos son importantísimo, saber actuar en todo momento, …. yo le dije que era importante porque en el nexo de unión entre el usuario y prestatario. Cuando hablo de usuario y prestatario me refiero a cliente empresa , y en este sentido, tiene que haber un punto de salida de entrada y esto es importante. Esto es igual que si hay una ley y un reglamento, yo creé el convenio de colaboración en el 2014. Un convenio de colaboración permanente y una comisaría con 5 Mossos d'Esquadra. ¡Qué suerte tuve! Aunque tampoco hay que decirle suerte porque la alerta 4 no es ninguna suerte, pero cuando se potencian los riesgos se potencian las amenazas y hay más recursos a disponer.

Otra cosa que también pasa….. es que la seguridad no tiene que estar cuando algo pasa, nos tenemos que anteponer, es este concepto de prevención y de salvaguarda que es importante

este es un tema de cultura de seguridad y de mentalidad. A la pregunta que me has comentado anteriormente. Un departamento de seguridad lo tienen que llevar grandes profesionales que son personas que estudian su trabajo y que valen que puede ser un guardia civil, un mosso, ... pero no porque sea un mosso o Guardia Civil ya está capacitado para hacer esto.

También te digo que si tengo que hacer una gestión o ir a la comandancia y veo un mosso un policía y me conoce la gestión será mucho más fácil.

Ya, pero te ha costado hacer contactos nuevos, porque los ds que no vienen del ámbito policial me dan este argumento, ...?

Mira los contactos son personas, y son amistades y las amistades tienen que ser sanas… a mí personalmente me gusta conocer personas, y dentro del sector de seguridad conozco personas en todos los cuerpos policiales. He salido de un cuerpo pero siguo siendo el mismo, Yo soy el mismo Guardia Civil de antes. Un buen profesional no tiene que cambiar su personalidad para nada. Esto sí que te lo digo yo, soy el mismo guardia, el mismo cabo, el mismo sargento, la misma persona que estaba de director en el Museo Picasso, el que fue a Bosnia. Me mato por hacer un favor a un compañero. Si no nos ayudamos entre nosotros con la que está cayendo, ... ¿quién nos va a ayudar?. Lo que pasa que soy una persona realista y coherente y sensata. Soy muy legal y me gusta ser legal, Enseñar las manos y si me equivoco decirlo. ¿Qué es lo que pasa? Que el rédito de todos los años de todos estos años... tengo muy buenos amigos de todos los cuerpos policiales. Pero yo sé lo que le puedo pedir y lo que no le puedo pedir ojo. Lo que pasa que después cuando llegué aquí con mis funciones de Director de Seguridad, dentro del espectro inteligencia…….

La seguridad es una ley y un reglamento desde el punto de vista de qué me dice lo que tengo que hacer... Pero a mí no me interesa eso. A mí no me preocupa el robo el hurto o el robo con fuerza a mí lo que me preocupa es un tío que venga aquí que me ponga un artefacto explosivo. Esto es lo que me interesa y para esto necesito… porque los directores de seguridad estamos dejados de la mano de Dios... el día 21 tengo q ir a Madrid a todos los directores de seguridad para hablarnos del tema de yihadismo. … Necesitamos ayuda, información, usted policía tiene que confiar en mí. Porque usted y yo estamos dentro de la misma família. Aquí no hay personas de primera ni personas de segunda, usted y yo sumamos yo también soy un profesional de seguridad. No hay una balanza que indique lo que es suyo y lo que es mío. ¿qué hago yo aquí? Yo trabajo con los Mossos d'Esquadra en una región central y los mejores Mossos

que hay en esta región los tengo yo siempre digo lo mismo. Cuando yo estaba en el Picasso eran los del sector de Picasso. Tengo que confiar las personas.

Yo cada semestre me veo con el comisario, cada mes me veo con el director,... yo necesito un nexo, no una amistad para irme con el de copas, las copa me las tomo en mi casa cuando quiera tomármelas, no de servicio. Yo con ellos hablo de seguridad de conceptos de valores y necesito que mi Sitio qué que la imagen de Montserrat se vea perjudicada por mí comportamiento. Por esto qué es lo que hago?? lo primero que le digo es vaya marrón que tienes teniendo Montserrat dentro de tu ABP no te lo puedes ni imaginar. Porque todo lo que pasa en Montserrat se multiplica por 4. No te puedes imaginar lo que genera todo esto, por esto hay que llevarse bien … Con un nexo de confianza. Pero siendo legal, yo sabré en todo momento lo que te puedo pedir, y tú sabrás lo que me puedes pedir a mí. Y si soy un buen profesional no puedo pedirte lo que tú no me puedes dar.

Por esto yo he creado gente aquí gente amiga, desde el punto de vista del respeto. Yo cada día me reúno con el caporal que hay aquí asignado. Después aquí hicimos una cosa muy importante, y luego hablaremos del concepto Montserrat de cómo se trabaja aquí….. una vez al mes nos reunimos todos los que trabajamos en Montserrat en materia de seguridad del SEM, Mossos, el director de seguridad etcétera. Estamos haciendo cosas muy buenas desde la bondad desde el respeto desde la conciencia y esto es muy importante. Yo por ejemplo, con los mandos que hay me llevo bien pero claro yo trabajo con el de la ABP de seguridad. Pero claro quién hace la inteligencia? El grupo de inteligencia .Yo tengo aquí gente de mossos muy interesante, ……. Yo cada día puedo recoger cosas que no me gustan, …. Yo tengo por ejemplo aquí un hotel y poder coger mucha información y lo que no puedo hacer es ponerme nervioso cada vez que vea algo raro yo tengo que hacer mi propia inteligencia. Yo trato mi inteligencia la meto en mi coctelera: información, poder, conocimiento la meto en mi coctelera y con la confianza que tengo en un señor brutal le digo mírame esto y hacemos inteligencia. Si sale la gestión positiva las habrá que el Señor de la ABP que la tenga que saber desde el primer momento pero el 90% es información que no es positiva. Vamos a crear una inseguridad? cómo se trabaja eso? Con cabeza,....

Esto se llama de inteligencia y yo lo he hecho durante muchos años. Yo en los cuerpos policiales perdona no puedo explicarte todos los sitios ni especialidades pero ya te puedes hacer una idea.

Para mí uno de los pilares de la seguridad es la ciberseguridad. Es que la sociedad se produce una situación paradójica y es que utilizamos más que nunca la tecnología pero no hay una cultura de seguridad de lo que hay detrás de esta tecnología. Mi niño coge la tablet, la juventud de hoy en día están enganchados a las redes sociales pero hay un desconocimiento brutal en cuanto es el background de lo que hay detrás de todo esto. Esto lo sé porque antes de ser policía estuve 10 años trabajando en aspectos tecnológicos en el departamento de sistemas y realmente no hay una cultura de ciberseguridad o de la seguridad de la tecnología me da igual. La seguridad no sólo es el vigilante de seguridad y la cámara de seguridad desde mi punto de vista el director de Seguridad cada vez apuntaré a un perfil mucho más técnico, que sepa hablar hablar de un con un lenguaje de ciberseguridad de inteligencia, y si no estás de acuerdo me encantaría que me lo dijeras ….

Seguridad ha existido toda la vida, toda la vida. Cuando yo vine aquí y me dijo un señor y me dijo un señor usted sabe lo que es el código Hammurabi, ahí es cuando se empieza a hablar de seguridad… La inteligencia lo bueno que tiene es la confianza que te da para decir las cosas. Ahora estamos en una seguridad preventiva. Antes de la época del Neolítico se hablaba de la seguridad defensiva ahora vamos con tecnología y antes íbamos con flechas.

Viendo Jerusalén vemos cómo las ciudades se defendían con sus murallas y este es el concepto del abanico de la terminología de la seguridad Vamos a ver, los planos los planes estratégico siempre han sido militares. Ciberseguridad viene la palabra ciber y seguridad. Mucha gente también habla de la videovigilancia desde cuando las cámaras vigilan, las cámaras graban y observan el que vigila es el es el operador lo que pasa que el marketing queda muy bien decir la videovigilancia pero claro me está ofendiendo usted está mi, que yo no sé nada de seguridad, pero quiero conocer cada día algo más. El proceso de i+d+i ha existido de toda la vida. Aquí se ha dado mucho auge a todo, ¿qué ha pasado últimamente? que antes cuando yo iba con mi Olivetti 98 y con su calco era de puta madre y los atestados les encantaban a los jueces. Ahora es diferente porque la tecnología me ha dado unos recursos para avanzar. Ahora hablamos del ciber que esto puede ser ciberdelincuencia ciberterrorismo puede ser de todo por esto cuando tú hablas de ciberseguridad es una seguridad integral que yo le llamo una seguridad integral de la información y toda la información tiene que tener una formación que ahí es donde estamos. Estamos avanzando demasiado, no dejamos hacer el proceso que se haga. Estamos con las cámaras analógicas y de repente aparece las cámaras y pegar a todos diferentes. La tecnología

va avanzando. Necesito Big Data permanente desde hace muchos años, el Big Data es una coctelera: INFORMACIÓN PODER CONOCIMIENTO, …….. una coctelera de información. por Que los guardias civiles han cogido a tantos etarras ?Te lo voy a explicar. De cada día de ir cada día a un sitio a otro hablar con todo el mundo de picar piedra y poner el puzzle de la seguridad mediante la información con lo que me ha dicho la señora del kiosco que me ha dicho que ayer vi una matrícula determinada, ….. eso es información información poder conocimiento. En el concepto de ciberseguridad, siempre ha existido la ciberseguridad lo que pasa es que ahora le damos el nombre. Porque la ciberseguridad la vemos desde el punto de vista desde el avance tecnológico.

Te voy a explicar un ejemplo que te va a gustar:

Yo en Montserrat puedo tener una horquilla De 10000 personas al día. Y esto no es la Sagrada Familia que me he entran todos por una puerta y me salen por la misma. ¿Qué es lo que me interesa?, los comportamientos no verbales, el concepto de la Seguridad en lo que respecta a la formación de la inteligencia. El tener unas cámaras en las crías están trabajando con algoritmos,... Una máquina es una máquina y después vienen las personas. Primero te diré que la ley 5/2014 ha traído una cosa muy importante porque antes las medidas de seguridad eran de tres tipos y ahora son de 5. La seguridad según la ley son: la seguridad organizativa, lógica, física, humana, y de la información. estos son los cinco pilares que yo tengo para ser director de seguridad. dentro de la tecnología, y de su avance, ¿qué es lo que necesito yo de la tecnología para que me ayude?. ¿la tecnología lo hace todo? No, un detector te avisa pero si no hay un tío que apague el fuego que se quema todo. Lo que necesita es implementar desde el concepto de la cultura, negociar con la tecnología, tan importante es lo humano como lo tecnológico. Necesito inteligencia de la seguridad de la información que me de premisas… ¿qué me interesa? que cuando me venga aquí un tío que sude mucho que mueva la cabeza para varios sitios, haya un algoritmo que me advierta. Esto es lo que yo estoy haciendo en el análisis de vídeo. ¿Qué tengo que creer yo en la ciberseguridad o en la Seguridad? yo tengo que creer en la seguridad no en la ciber. En lo tecnológico todo avanza, tengo que entender que el informático tenga la misma cultura de seguridad que yo, que no la tiene. Al final todos vamos a la misma en los mismos caminos.

Por eso el proceso de inteligencia se realiza con tranquilidad, con un buen análisis de riesgo. Hay tres tipos de factores: el Factor estructural, los factores de riesgo factores de

protección. La ciberseguridad debería hacer esto: analizar el espacio que tengo, saber cómo está construido, qué riesgos hay en mi espacio y que protección le voy a dar a mi espacio para poder protegerlo, y en base a esto me sale una fórmula que me dice el riesgo que yo tengo.

Los riesgos se pueden reduir, se pueden transferir, se pueden aceptar y se pueden anular. Si tú no quieres que se cae que se caiga ninguna piedra de Montserrat, cárgate Montserrat. Eso no puede ser. Entendamos el riesgo sin obsesión, con cordura, y entramos una lista dinámica de lo que hay. Estamos avanzando muy deprisa no hemos terminado algo y empezamos otra cosa. Hay gente que habla de seguridad física y lógica y no tienen ni puñetera idea.. grandes profesionales que no tienen ni idea de lo que hablan. Este concepto de la seguridad siempre ha existido a nivel estratégico lo que pasa y ahora la tecnología nos hace avanzar de otra manera.

Déjame que te diga otra cosa muy importante si yo te preguntará ahora mismo a ti cuál es el riesgo que más te preocupa a nivel de todo? yo a esta pregunta te respondería que a mí el nivel 4 me preocupa mucho pero no es lo que más me preocupa. ¿Tú sabes lo que me preocupa? el Protocolo de Kioto, los riesgos ambientales, esto es lo que va a destruir todo el universo de este mundo. Quédate con esto que te estoy diciendo. El Polo Norte y el Polo Sur, las temperaturas las humedades las densidades los cambios bruscos cada vez en verano hace más calor y en el invierno menos lluvias quédate con esto. Ese es el mayor riesgo que tenemos lo que pasa es que así habla poco porque no interesa.

Hay mucha falsedad en todo hay países que están haciendo el juego a muchas cosas y en este sentido yo que he estado en inteligencia te puedo decir muchas cosas de lo que interesa y de lo que no interesa. Hay un país que no voy a entrar a nivel político sino a nivel de gestión de seguridad que me apasiona y es Israel. Y me apasiona porque tienen cultura de seguridad desde la mañana hasta la noche. Estos no te miran el coche sólo después de un atentado, …..

Por esto quiero dejarte claro una cosa, Que los avances son muy buenos pero la tecnología da mucho por culo,.. ojo con la tecnología. la seguridad 100% no existe ni al 100 ni al 90 ni al 80, ¿qué es lo que existe en seguridad? todo el mundo es terrorista? No, pero ¿cualquiera puede serlo? Sí. siempre hay que estar prevenido. Este concepto de prevención y la madera está en la que te estoy hablando quién lo tiene? dentro del segmento de seguridad lo tienen 4 personas. Es que mi seguridad es diferente a la del corporativo La Caixa? no, ¿sabes que cambia? que estos señores tiene una cantidad de recursos impresionantes y lo que estamos en sitios que casi no tenemos nada de nada….. en los que me dicen no entiendo cómo puedes estar un año con

2700000 personas y con estas cámaras… con experiencia, y con ingenio se puede estar y sobre todo con buena gente y formando buenos equipos de trabajo. Esto es lo que yo necesito del grado de seguridad de los que vais a salir.

Todo se aprende con formación, pero cuando terminas la formación tu trabajo es un aprendizaje continuo. ¿Sabes la cantidad de reglamentos y de normas que hay…. …?

Cuando yo digo que no tengo ni idea de seguridad es porque estoy aprendiendo de seguridad cada día y llevo ya 37 años. Y cada día aprendo algo nuevo y cuando no sé algo lo pregunto. Y lo bueno de todo es ser honesto, siempre hay que ser humilde. La palabra humildad no se dice, se hace. La excelencia es un proceso al que nunca se llega se va consiguiendo.

¿Como una persona consigue estar más segura que la otra? con conocimiento y yo te repito y te lo digo, cuándo Ana Aisa le dijiste lo que querías hacer.. ella habla cada día con muchos directores de seguridad el que ella me mandara a mí ese correo diciendo que había una persona interesada en un tema y ella pensará en mí fui la persona más feliz del mundo durante ese segundo. Cuando pasó este segundo ya dije tengo que seguir siendo coherente porque no me lo puedo creer, porque la conversación contigo terminará de aquí a 10 minutos y eso ya habrá pasado….

Lo que yo pido y lo diré a todos los profesores es que estos señores necesitan experiencia y la experiencia se consigue trabajando porque seguramente ahora mucha de las dudas que tendréis es a dónde iremos que opciones tenemos…

CAMBIA DE TEMA….

Falta mucha cultura de seguridad hasta los que están enseñando no la tienen. Aquí me he pasado un poquito pero déjame que con 36 años de experiencia… mi padre me dijo que a partir de los 50 no hablara mucho que hablara poquito. Bien falta mucha cultura de la seguridad

ESTA ERA LA ÚLTIM PREGUNTA, LA DE LA CULTURA DE SEGURIDAD

11.6 Entrevista José Luis Franco

FICHA TÉCNICA	
Descripción	Entrevista a José Luis Franco, director de seguridad Torres Mapfre
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector.
Fecha	14 de marzo del 2018
Lugar	Dependencias Torres Mapfre
Observaciones	

1.- **José Luis, no nos conocemos, y lo primero que me gustaría comentarte es tu trayectoria profesional. Cómo has llegado hasta aquí.**

Bueno, la base en la que se cimienta mi trayectoria es el mundo militar. Empecé como militar profesional durante 5 años en tres unidades diferentes. Empecé en Ceuta después pasé a Madrid a la guardia real y después aquí en Barcelona Operaciones especiales. Entonces aquí ya cuando empiezas a ver una salida y llevas este bagaje uno de los primeros caminos que buscas y además porque me gustaba, porque dentro de lo que cabe en el mundo militar lo habías hecho y una de las opciones que había era ser Guardia Civil, Policía Nacional etcétera y veías que era viable. Una salida rápida y similar en el mundo civil la encontré la seguridad privada. Empecé como vigilante y al año y medio me ofrecieron la posibilidad de irme a Diagonal Mar para abrir diagonal mar como jefe de equipo. Bueno para mí era un reto abandoné mi zona de confort y para mí fue un reto y yo creí que era válido para ello y lo probé y salió bien. Ahí estuve 7 años y después de ahí pasé a inspector de servicios dentro de la compañía de seguridad Securitas. Entonces ahí digamos que abandoné la operativa y me dediqué más a la gestión a la gestión de equipo, a la gestión de 258 personas y sus diferentes servicios, el trato con los clientes etcétera.

En esta etapa ves un poquito la seguridad desde o por decirlo de otra manera los toros desde la barrera. Dejas el mundo operativo, y estás más a la gestión de los operativos. A mí esto no me acababa de cuadrar y me ofrecieron irme como director de seguridad del Centro de Cultura Contemporánea de Barcelona qué es un consorcio de la Diputación y Ayuntamiento de

Barcelona. Fueron 10 años brutales aprendido un montón, es un centro de cultura que digamos era un cajón desastre de lo que es cultura espectáculos de pública concurrencia, de salas, … y acabas tocando dentro de un mismo servicio muchos campos. Aprendí un montón porque una de las primeras cosas que tienes que tener clara es que siempre estamos aprendiendo y tienes que tener esta humildad para decir quiero aprender quiero aprender enséñame, aunque a nivel jerárquico esté por debajo tuyo. No se tienen que caerte los anillos a la hora de aprender de los que ya llevan más tiempo y fueron 10 años la verdad que fabulosos. En esos 10 años llega un momento que a través de… se me ofrece la oportunidad de venir a hacer como director de seguridad y las condiciones eran muy buenas, y las acabas aceptando también como otro reto cómo es la Torre Mapfre en este caso, un edificio emblemático de Barcelona, un edificio de gran altura, alta capacidad etcétera. En su día estuvo dentro de las primeras amenazas de Al Qaeda y lo acabas cogiendo como un reto personal. Lo que sí es cierto es que en el Centro de Cultura todo era cíclico eran los mismos eventos repetidos cada año. Desde que era pequeño y piensa soy joven y tengo aspiraciones y quiero progresar entonces acepté el reto y la verdad es que de momento somos un equipo de 4 personas, una gerencia de 4 personas y es apasionante y muy bien la verdad.

2**. No es ningún secreto que los puestos de director de seguridad están capitalizados por miembros o ex miembros de los Cuerpos y Fuerzas de Seguridad. ¿a qué crees que se debe todo esto?**

Aquí hay dos factores clave para mí y siempre lo he dicho. El primero la creencia y a veces falsa creencia de que lo publicó se puede comparar a lo privado y entendiendo que a lo mejor un policía sabe la gestión de un edificio porque es algo… en teoría es seguridad etcétera y realmente yo creo que no y he conocido grandes profesionales que vienen del Mundo de la seguridad pública y son fantásticos directores de seguridad. Pero hay otros que no, tú gestionas recursos limitados y con estos recursos tienes que dar la máxima protección es muy importante COMO EN EL AJEDREZ, tener todos los campos cubiertos Y TEJER UNA ESTRATEGIA. Los análisis de riesgo para nosotros son importantísimos saber cómo cambia el panorama tanto a nivel podríamos decir terrorismo internacional geopolítica porque hoy en día cualquier cosa que pase por ejemplo en Afganistán nos puede repercutir aquí, ¿por qué? porque tenemos tropas allí, por ejemplo. Un ataque de nuestras tropas puede generar una amenaza contra el pueblo español etcétera. Todo esto, la criminología también, lo modus operandi, son básicos para poder estar

al día en lo que quieres implantar en cuanto a seguridad. Esto en la ser. pública no será tanto como la seguridad privada. Aquí los recursos son importantísimos, tú tienes que responder cuenta de resultados y en la seguridad seguridad pública no es así.

Después por otro lado y esto sí que nos hemos encontrado que lo que se contrata es la agenda de contactos y la capacidad esa persona dentro del cuerpo policial al que pertenecen de moverse. Esto sí que a veces es digamos que va en detrimento de una persona que tiene grandes cualidades para ejercer, pero a lo mejor no tienes tus contactos y no era tan fácil a una Brigada de Investigación o una DIC para mover hilos.

Luego la gente al final, la que no viene del mundo lo que me dice es que no le cuesta tanto hacer contactos, que existe una predisposición

Sí, pero muchas veces no te equivoques esta predisposición es muy limitada yo puedo conocer al intendente y tú pregúntale algo a este intendente algo de que a ti te interesa la información…… a mí lo que me interesa aquí es por ejemplo si hay un grupo organizado que se dedica a reventar coches… yo tengo un parking que gestionar. Dime qué matrícula y que personas estás buscando. Dame una información que a mí me ayude a tomar medidas y que de alguna manera poner mis recursos al servicio de prevenir los actos de estas personas.

Esto no nos lo encontramos esta bidireccionalidad de la información.

Esta relación la ha marcado de alguna manera la ley. La del 92, situaba la seguridad pública por encima de la privada. Esta relación la ley del 2014 la sitúa en una relación de complementariedad, … pero de lo que todo el mundo habla, desde el sector privado es que no hay una confianza desde el sector público hacia el sector final, …

Bien, es así entonces lo que pasa que al final siempre es que va más a las relaciones individuales. Al final acaba siendo fulanito de tal con fulanito de tal qué ha sido intendente y que ahora es director de seguridad, pero esto…... y mira que la nueva ley lo posibilita esta posibilidad de compartir información… que siempre que sea necesario para la seguridad ciudadana el compartir esta información. Esto ya queda recogido en la ley, pero claro una de las preguntas que yo le hago muchas veces a los intendentes es que si es conocedor de los servicios de seguridad que tenía su abp. Él me dijo una serie de servicios, pero se dejó un montón y lo que estaba perdiendo ¿qué era? La capacidad de información que estos servicios pueden generar y que él dejaba escapar o que se deja escapar por no tener un feedback o una relación con esta persona a nivel toma mi email si ves algo raro llámame. Al final tienes antenas en todos lados y

repetidores que se traducen en información que si tú le preguntas una información te la pueden devolver esto al final se basa en la confianza.

Esta confianza se tiene que trabajar muchísimo. Ahora mismo tenemos un montón de sitios y de servicios porque piensa que la seguridad privada tiene muchos más recursos que las pública por esto sencillamente lo que tienes que hacer es aprovecharlos. Al final muchas acciones delincuenciales tienen lugar en lugares donde hay muchos circuitos de video vigilancia y es una pena que esta información se pierda por no haber esta facilidad…. sí que es cierto que se abierto la unidad permanente operativa la UPIOC, pero al final si dejas todo el peso de la relación de vigilancia de vigilantes de seguridad de directores de seguridad en una sola área cómo es la policía administrativa en lugar de pasarlo a todos los grupos operativos que tenga la capacidad de gestionar vosotros las redes dentro de vuestra demarcación ... algo tan sencillo como esto

3. ¿Cuáles son las amenazas a las que te enfrentas cuáles son tus preocupaciones y cómo haces frente a todo esto?

Las amenazas hoy en día son muy cambiantes, las tienes que analizar detenidamente, y una de las funciones del director de Seguridad es hacer un análisis de riesgo constante incluso el análisis DAFO, ver sus debilidades sus fortalezas, oportunidades y las oportunidades que tiene el enemigo. En el mundo militar decimos que toda táctica pasa por saber cuándo cómo dónde y por dónde. Si yo tengo explicaciones o respuestas hasta 4 preguntas perfecto, pero generalmente por decirlo de alguna manera el enemigo siempre va por delante nuestro. Yo puedo tener contestación a 3 pero siempre habrá una que no la tendré. Entonces los análisis de riesgo pasan minuciosamente, … como te decía antes son costes también, porque la seguridad tiene un coste tiene un nombre, entonces cuando tú haces un análisis de riesgo tienes que tenerlo muy claro dónde o por dónde te puede venir el daño o la amenaza. Intentar blindar estás oportunidades con medios tanto humanos como electrónicos y sobre todo evolucionar estos medios lo que hoy es válido a lo mejor mañana ya no porque hay una nueva amenaza. Entonces tenemos en cuenta también el nivel de alerta terrorista en el que estamos nivel 4 sobre 5. El nivel de amenaza en cuanto a un autor que antes, cuando hablábamos de ETA eran un grupo totalmente organizado con una estructura clara con una orden jerárquica clara, con unas órdenes para atacar no era una barra libre. Hasta que el órgano directivo no daba la orden no se podía atacar y eran objetivos y un modus operandi diferente avisando antes de actuar. Ahora pasamos a un terrorismo totalmente … hasta ciertos años desconocido para todos

incluso para las Fuerzas y Cuerpos de Seguridad que han tenido que ponerse las pilas y sobre todo se trata de un individuo que lo tenemos por aquí que está andando por la calle que está andando con nosotros que convive con nosotros que está a nuestro lado y que sabemos que en un momento dado esta persona pueda actuar. Personas que cada vez están sometidas a un proceso de radicalización más rápido cada vez y mañana nos viene con un chaleco lleno de TATP. Todo tienes que evaluar tienes que atender, pero también tienes que entender que debes dejar libertad a la gente. Y si tú te blindas y contra más medidas hagas están ganando ellos porque al fin al cabo es lo que quieren. Entonces tienes que ser un poco……. ese riesgo o ese tanto por ciento de riesgo lo vamos a tener y tienes que ser flexible en las medidas de acuerdo al riesgo que tú recibes por esto es muy importante yo cada vez lo recalco más, la inteligencia en la seguridad privada. y cuánto dices que es inteligencia en seguridad privada no es una seguridad no es un director de Seguridad Privada muy listo. Estamos hablando de convertir datos en información y la información en inteligencia y la inteligencia son armas que te permitirán ir por delante y anticiparte la Comisión del riesgo. Hoy tenemos lo que son fuentes abiertas EL osint, esto es súper importante. Todo esto lo tienes que enfocar de alguna manera recibir todos estos datos, estar al día de todos estos datos, e incluso disponer de herramientas como por ejemplo la creación de perfiles falsos que te permite recibir información y ya no solo me refiero al terrorismo sino a la gran masa social que tenemos en la calle o a los grupos anti sistemas. El momento político que estamos viviendo actualmente en Cataluña, todo esto puede traducirse en una manifestación aquí delante que me corté el tráfico de la entrada del parking. Si yo me he dado cuenta de esta información se lo que ocurre puedo cerrar esta entrada y entrar por la otra. Esto con un sencillo Twitter que he visto de Aran o de quien sea. Todas estas herramientas todo el día son válidas y sobre todo la gestión de recursos. Cuando vamos a dirección y vamos a pedir dinero para nuestro departamento es muy importante no vender humo lo primero, más que vender hay que convencer. Más que decir que puede venir un avión y nos va a tirar la torre abajo o como no, puedo entrar una furgoneta y volarnos el el parking, … pero vamos a ANALIZAR los riesgos que hay y qué medida que me permitan vivir en un estado democrático. Abraham Lincoln cuando le decían que le iban a matar había una frase con mucha cabida en el mundo de los escoltas… que le decían métase en casa que le van a matar y él dijo…. podréis meterme en una caja fuerte y no me matará nadie, pero dejaré de ser el presidente de los Estados Unidos. Tenemos que hacer nuestro día a día con esta amenaza y convivir con ella, pero

sobre todo analizando la día a día, viendo sus mutaciones y tomando medidas nosotros al respecto.

4. **Has sacado un tema que venía después, pero me viene genial y es el tema de la inteligencia. Me has dicho qué es la inteligencia y me has dicho que es el valor añadido de la información que permite anticiparte. La información es poder y si la inteligencia te da información te da el poder de estar por encima del otro y aquí es donde voy y lo quiero reaccionar con la relación público privada y la teoría que yo tengo. Lo que me está llegando es que a través de la inteligencia la parte del sector privado tiene más información o información de primera mano sobre todo también en gran parte por las comunidades de inteligencia, de grandes corporaciones de inteligencia… con lo cual está llegando mucha información antes al sector privado y el sector público. Entonces creo que de alguna manera esto va a cambiar la relación que hablábamos antes y ahora dejemos al margen la confianza creo que el poder que da la formación acabará situando por encima al sector privado básicamente por un tema de recursos porque podrá pagar grandes analistas de inteligencia y esto el sector público hoy por hoy no se lo puede permitir no puede alcanzar. ¿tú crees qué esto va a cambiar el modo en el que se va a trabajar a partir de ahora?**

Yo creo que sí y de hecho ya está cambiando. Sólo tienes que ver como por ejemplo empresas de seguridad privada antes su concepto era contratación de vigilancia y sistemas. Póngame un vigilante en el edificio y cuatro cámaras. ahora cada vez más ofrecen servicios de inteligencia, ofrecen servicios de vigilancia virtual de ciberseguridad etcétera, … porque por que venga el riesgo está ahí y dónde hay riesgo hay cuota de mercado entonces ahí es donde quieren y dónde vamos a ir la mayoría de servicios de seguridad. La Sagrada Familia, la hemos visto amenazada por Daesh y ahora tiene que convivir fundamentalmente con los servicios de información policial y la Sagrada Familia genera la información que después se podrá convertir en inteligencia a través de su circuito cerrado de televisión, a través de las amenazas que reciban redes sociales etcétera. Todas estas amenazas y esta información se ha de poner en valor tanto por lo público como por lo privado, pero sí que es cierto que la información primero, la inteligencia, y la información caduca. Lo que ahora es válido mañana no es, lo que sí yo lo pasó en estas primeras horas permite detener una amenaza si lo paso más tarde la amenace se cumple. Después también ¿qué es información? ¿qué sirve para información? si generamos mucha información sí o sí vamos a tener que dotarnos de analistas qué conviertan estos datos en inteligencia y esto

no es una tarea fácil. Ahora mismo los recursos privados y cada vez más grandes corporaciones y empresas de seguridad privada ya están incorporando analistas de inteligencia. No solamente por el tema de su vida privada sino por el tema económico para tejer la estrategia económica y anticiparte a tu competencia … o ir a una reunión con un cliente con más información que él te permite jugar mejor las cartas. Los directores de seguridad tenemos que ser conscientes de que el pilar fundamental de la protección pasa por la inteligencia. Saber con quién compartir la inteligencia que tú generas, saber de quién recibir inteligencia. También hay que tener en cuenta que una mala inteligencia te llevará a producir errores. Yo que la inteligencia es importantísima y generamos más que la pública. Hoy en día las empresas privadas ya tienen sus departamentos de ciberseguridad. Las empresas privadas cada vez se dedican más a la seguridad cibernética, al análisis de riesgos sobre EL osint que se genera en un determinado servicio.

Hoy en día las empresas van a tener que dotarse de sus propios analistas y no dotarse de los analistas de los de las empresas de seguridad privada porque al fin y al cabo nos pueden dar una información sesgada porque al final cobran de ti. Al final deberás tener a los tuyos que te cree esta figura

5. ¿**cómo tienes integrada esta figura en tu empresa tienes una persona dedicar a esto?**

No, ahora mismo no. Somos todos lo que estamos haciendo esta tarea. Sí que tenemos un punto muy bueno y es que la compartimos lo que a mí me llega por un punto yo lo comparto con otra persona y ella me la devuelve diciendo oye eres la cuarta persona que me dices lo mismo etcétera. Lo que sí que tenemos un problema es que las redes sociales hoy en día lanzan una serie de bulos y al final acabamos diciendo siempre del mundo la inteligencia es que al final es tan importante saber cómo saber quién sabe y al final te tienes que acabar rodeándote de fuentes fidedignas. Y al final también acabamos teniendo nuestros contactos en las Fuerzas y Cuerpos de Seguridad y a veces también nos referimos a agentes rasos. Ahora te decimos yo tengo un contacto que es intendente… a lo mejor yo tengo 3 que son agentes y me sacan más información….

5. Hemos hablado de ciberseguridad, por lo que respecta a la ciberseguridad desde mi punto de vista creo que es uno de los pilares fundamentales de la seguridad privada porque al final te permite proteger toda tu información en una sociedad de la información como la de hoy en día. Lo que es curioso, lo que sucede con la ciberseguridad, yo al final tengo mis teorías para

para todo y me gustaría que me dijeses qué te parece, pienso que estamos en una sociedad que cada vez depende más la tecnología no sé si eres padre o no, pero por ejemplo mi niño se utiliza la tablet, están dependiendo de la tecnología. Avanza la tecnología, pero no avanza o se queda estancado la concepción de seguridad de lo que lleva esta tecnología, qué es lo que hay detrás de esta tecnología. Por mi experiencia anterior antes de ser policía trabajé en una empresa de servicios el Departamento de Sistemas de la Información y no había cultura de la seguridad en temas de ciberseguridad. Esto explica en cierta manera esta falta de cultura, cómo la ciberseguridad se está llevando desde los departamentos de sistemas y no des los departamentos de seguridad. Esto es una gran crítica y para mí es una pena porque no cabría en la cabeza de nadie que una empresa se auditara a sí mismo porque el resultado va a ser el que es. Entonces, de alguna manera esto lo extrapolo al mundo de la seguridad y me choca mucho esto. ¿Cómo es posible que nos esté llevando la ciberseguridad desde los departamentos de seguridad??

Sí sí, cada vez más vamos a esa …. y se está convirtiendo en una digamos en una separación total de la seguridad física de lo que es o lo que debería ser la información que es el mismo es el bien más preciado que tiene una empresa. si me roban el ordenador ya no es el valor del ordenador sino el contenido de este ordenador. Entonces yo creo que efectivamente estamos pasando por alto y dejando en manos de grandes profesionales de la tecnología, pero no profesionales de la seguridad o defensa por decirlo de alguna manera y ahí tenía que haber unas sinergias y una colaboración estrecha y sobre todo que crear este departamento de seguridad de cualquier corporación que debe depender del director de seguridad y que se hablen y que se lleguen a acuerdos para proteger la información etcétera.

Este lenguaje del mundo de las IP y de la seguridad pura deben encontrar a un sitio para converger.

5.1 De alguna manera ya no es un tema solo a nivel de vigilancia sino de normativa ISO... tú para instalar determinadas cámaras de seguridad la ley te dice muy claramente cuál es el mínimo y qué es lo que tienes que cumplir. Esto en en ciberseguridad también existe. Existe normativa ISO desde qué tipo de firewall tienes que poner etcétera. Esto, desde mi punto de vista no se puede hacer de un sitio que no sea el Departamento de Seguridad.

Una de las personas que he entrevistado en este sentido me ha hablado de un perfil más técnico por lo que respecta a la figura del director de seguridad. Una persona que sepa hablar

de inteligencia y en términos de ciberseguridad porque al fin y al cabo es la persona que deberá rendir cuentas al CEO o a quien sea. ¿Cómo ves tú o hacia dónde crees que va a girar la figura del director de seguridad?

Yo creo que va a ir hacia ese punto y sí que es cierto que hay que ponerse las pilas y trabajar y sobre todo dotarse de conocimientos porque en un mundo de la información el robo de información el proteger la información a nivel corporativo incluso a nivel reputacional como tú bien decías aquí coincido totalmente contigo, El departamento de Seguridad tiene que integrar la ciberseguridad y la defensa de la Corporación y los datos de la corporación. entonces el director de Seguridad sí que tiene que cambiar creo que sí a ese perfil qué es una persona que entienda y sepa y le de valor a la inteligencia como medida de protección primera importantísimo, y segundo que sepa entienda y hable el lenguaje de la ciberseguridad y que cuando haga unas medidas o cuando vayamos a instalar un circuito cerrado de televisión que vayamos por IP que protejamos estos datos a qué servidores se va la información como protegemos los servidores todo esto yo creo que es el futuro y cada vez avanza más rápido con lo cual cada vez llegamos te hace forma y tienes estos conocimientos. Te lo exige el mercado laboral cada vez más rápido.

6**. Imagínate ahora que eres el director de recursos humanos y el CEO te encarga contratar un director de seguridad y tienes que buscar un director de seguridad. ¿qué buscarías en un director de seguridad?**

Así rápido es complicado, pero primero una persona resolutiva. Hay una serie de cualidades que, en todos los trabajos, pero no un director de seguridad más tiene que ser una persona despierta ágil que sepa dar soluciones rápidas que tenga la formación para dar soluciones rápidas. Alguien que tenga esta capacidad de en un momento que recibe una llamada advirtiéndole de un problema él sepa dar soluciones al problema, que conozca muy bien cuáles son los factores claves de la seguridad y después a nivel de estudios sí que es cierto que cada vez más lo que tú decías. Este director de Seguridad debe venir complementado con algo ya no vale eso de yo tengo la TIP de director de Seguridad o soy policía y ya está. Tiene que venir desde un punto de vista tecnológico e incluso en departamentos desde un punto de vista criminología derecho son carreras que te ayudan a ejercer de una manera más fiable y sobretodo tu profesión ya no vale la Tip y sobre todo esa evolución técnica. Yo creo que cada día será más demandada e incluso cada vez tiramos que el director de Seguridad ha dejado de ser aquella persona vetusta con

bigote y gafas para pasar a ser una persona despierta y ágil que habla de tú a tú cuándo estás en un congreso lo que sea te habla de tú a tú de una manera muy sencilla fácil y tiene conocimientos un poco de todas las vertientes de la seguridad integral entendiendo por seguridad integral cabe es el abanico más amplio.

7. **La última pregunta tiene que ver con la cultura de seguridad de cómo debe transmitir el director la cultura de seguridad no solo a tu departamento sino a todo el resto desde abajo hasta llegar hasta arriba.**

Esto es vital desde el CEO, que entienda que no quieres un recurso valioso y que eres una inversión que tú estás invirtiendo en seguridad porque la seguridad si la vamos a buscar la pirámide de Maslow la encontramos enseguida…. que está ahí con lo cual es algo que necesitamos para proyectarnos hacia arriba hacia algo mejor. Esta pedagogía de seguridad pasa desde el CEO hasta el último visitante que entra por la puerta del centro que proteges hasta el último…. desde que le das las hojas de bienvenida hasta que informas del PAU. Todos estos inputs que vas dando continuamente que tienen el objeto de que la persona se sienta seguro ocupando el puesto de trabajo que ocupa esto es algo diario es una pedagogía continua que de vez en cuando la tienes que tensionar porque estamos en un país que nos bajamos muy rápido hace poco hemos sufrido un atentado y a los tres meses parece que no haya pasado nada ya nadie se acuerda y cuando intentas poner una medida a veces la gente reacciona diciendo qué bruto. Este riesgo lo cubres formando y tensionando a esos equipos de gente con charlas de formación para que entiendan que es algo necesario.

Nosotros trimestralmente vamos haciendo reuniones con todos estos departamentos incluso con los clientes explicando los planes de autoprotección que hoy en día es nuestro mecanismo de defensa donde yo voy recogiendo los riesgos desde el medioambiental, el terrorismo incluso cada vez más en los simulacros tienes que ir a morir al riesgo que supone el terrorismo.

11.7 Entrevista Joan Miquel Capell

FICHA TÉCNICA	
Descripción	Entrevista a Joan Miquel Capell, Director de seguridad de la Diputació de Barcelona.
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector
Fecha	21 de -marzo del 2018
Lugar	Diputación de Barcelona (Dept. Seguretat)
Observaciones	

1.- Sr. Clapell, no nos conocemos … la primera pregunta me lleva a saber más de ti. ¿Cuál ha sido su trayectoria profesional hasta llegar a estar donde estás..?

Yo, ... yo he estado 31 años en la seguridad pública en todas las categorías de Mosso hasta llegar a ser comisario. Ha sido una parte de mi vida muy satisfactoria. He tenido un contacto con el mundo de la seguridad muy intenso y por decir de alguna manera de la seguridad de puertas hacia fuera. La seguridad de la calle, de la montaña, relacionada con la convivencia de las personas entre ellas y de alguna manera y alguna vez he entrado en la seguridad de puertas hacia dentro cuando he tenido un asesinato, un muerto dentro de algún edificio... Dentro de los edificios y de las casas, dentro de las fábricas, la seguridad pública se ha excluido y digamos que no hemos sabido encontrar la manera de hacer seguridad aquí dentro.

Cuando ya he agotado estos 31 años de Seguridad Pública, que quería aprender algo más y ofrecer la seguridad de puertas para dentro. Es decir, cómo puedes ayudar a la seguridad pública desde la seguridad privada y desde la prevención. A lo largo de mi carrera profesional he tenido 11 consejeros y todos tenían un denominador común. Todos ellos, sus órdenes y sus prioridades políticas siempre han sido que querían más prevención y menos represión. Era una máxima política como un ideograma como una idea que ellos tienen y que el responsable de la seguridad pública le toca transformar esta ideología y manera de hacer en una operativa concreta de los policías. Yo lo que intente y lo que he intentado a partir del 2011 y 2012 fue crear la Comisaría General de mossos que se llamaba comisaría de Mediación de prevención de relaciones

institucionales y que tenía la voluntad de dedicar muchos esfuerzos policiales a la prevención . Transformar la voluntad política en operativa. La policía tiene unas unidades de investigación de orden público de tránsito pero no tiene ninguna unidad específica de prevención y la prevención hoy en día es algo transversal a toda la policía sin tener una unidad específica que se llame así. Está fue la idea con la que se creó esta comisaría de prevención.

Salí de la policía porque la Diputación me ofreció la oportunidad de realizar esta seguridad de puertas para dentro. Pero puertas para dentro de los municipios Y asesorando a los alcaldes y a los regidores en materia de seguridad pero lógicamente como los ayuntamientos sobre todo los más pequeños (313) en la provincia de Barcelona de los cuales la mitad no tiene policía local.

Por otro lugar la la Diputación como Administración Pública dispone de gran cantidad de bienes sobre los cuales tiene una gran responsabilidad de protección de sus personas y bienes de lo que yo hablo o me refiero de puertas para adentro y por lo tanto lo que se tiene que hacer es estructurar la planificación de la prevención de la seguridad desde la propia Administración Pública .Para que te hagas una idea de dónde de dónde estamos la Diputación de Barcelona dispone de unos 150 pisos propiedad de la Diputación y que hace falta ver cómo se protegen delante de ocupaciones ilegales y este tipo de cosas porque si no se hace esta prevención y estas medidas son eficientes pueden ser ocupados por delincuentes o por personas necesitadas O por alguien que no sabes quién es …

Por otro lado la Diputación dispone de otros programas como por ejemplo el que se conoce como el de las pulseras o collares de la gente mayor que viven solos y por lo tanto tenemos unas 75.000 personas con una pulsera de este tipo que cuando tienen un problema toca la alarma y por un sistema de megafonía hablan con la central etcétera y esto todo se gestiona desde la Diputación.

Utilizando com oexcusa estos dispositivos se ha picado a la puerta de casa de una persona mayor diciendo que era un técnico de positivo de alarma que venía cambiar la pila y se ha utilizado esta excusa para entrar en casa del domicilio de la persona mayor y robarle. A mí me ha parecido que es muy importante que la policía pueda encontrar al autor del robo con este engaño ….des del El Departamento de Seguridad intentamos pensar no cómo coger a este delincuente que sería más una cosa de Seguridad Pública lo que intentamos pensar es , ¿cómo podemos hacer que esté señor mayor no le abra la Puerta?. ¿Cuáles son los nuevos elementos de seguridad que hay que hacer servir para que esté Señor esté seguro en su domicilio… Por

ejemplo colocar detectores de humo en la cocina para estas personas que están solas conectados a la misma sistema de alarma para hacer que esta alarma se activa sola en el caso de que la persona no lo haga o lo mismo si la persona mayor no abre la nevera en 24 horas o no ha tirado de la cadena del váter.

En definitiva, es pensar medidas de puertas para dentro para que puedan ayudar en la seguridad tanto pública como privada.

Como tú decías muy bien la Diputación o el papel del director de seguridad en la Diputación de Barcelona es Es un papel desde el que se gestionan 135 vigilantes de seguridad de empresas privadas y unos 30 auxiliares de empresas privadas de seguridad. Al hacer esto me pareció que era imprescindible para mí obtener la habilitacion del Departamento de Interior del Ministerio del Interior español como director de seguridad para poder dar instrucciones a los vigilantes de seguridad. Realicé las pruebas pertinentes y obtuve mi habilitacion para poder dar las instrucciones a estos vigilantes que tenemos, para vigilar espacios de los recintos la Diputación. La Diputación de Barcelona tenía dos Cuerpos de Seguridad Pública qué vigilaban sus instal·lacions. Por un lado el cuerpo de vigilantes y por el otro los Mossos d'Esquadra. A partir de la ley Orgánica 1986 se decide que no puede haber policías provinciales y a partir de 1983 el cuerpo de los Mossos d'Esquadra pasa a la Generalitat . A partir del 1986 Y después de las sentencias respectivas a partir de 1992 la Diputación de Barcelona que tenía dos cuerpos de vigilancia Pública pasa a no tener ninguno y lo que hace es contratar empresas de seguridad privada. Por lo tanto, lo que tenemos que hacer es contratar empresas por el procedimiento que nos sea más útil y eficiente. ¿Qué es lo que pasa en estos momentos?. Que al cambiar la Ley de Contratación el director de seguridad lo que tiene que estar es al tanto de todos los cambios y conocer cómo funciona el sistema de contratación más allá de lo que hacen los propios vigilantes y también conocer toda la normativa referente a la protección de datos que entra en vigor el 25 de mayo. Tendremos que tener en cuenta la protección de los datos de las personas a través de los vigilantes y ver cómo se tratan los datos de carácter personal de las personas.

2.- **No es ningún misterio ni secreto que los puestos de DS los están ocupando en un gran porcentaje ex-miembros de cuerpos de fuerzas y cuerpos de seguridad del Estado. ¿A qué crees que se debe, ¿cuál es su valor añadido?**

Yo creo que la seguridad pública, y las personas que han trabajado en la seguridad pública tienen una parte de formación impartida en las escuelas de policía Guardia Civil, Mossos,

etcètera... Una formación en materia de seguridad que es una formación que le hace más o menos óptima para dirigir personas y para dirigir personas que van a armadas y al mismo tiempo cuando uno ha trabajado a la seguridad pública y ha ido subiendo por las diferentes categorías ha tenido que gobernar o dirigir personas que se han encargado de la seguridad de un espacio, de un de un edificio de algún lugar y esto les da un perfil que los hace óptimus para poder dirigir también a a vigilantes de seguridad. Por otro lado estas personas muchos de ellos han tenido otras inquietudes y han seguido formándose y gran parte de ellos son criminologos. Hay mucha gente de la seguridad pública que han ido a las universidades a formarse en materia de criminología entonces estas personas que han tenido estas formaciones y estas inquietudes muchos de ellos en la medida que las universidades han abierto las posibilidades para formarse como directores de seguridad y han ido a las universidades ampliar estos conocimientos como directores de seguridad. Después es lógico qué estas personas han ido a buscar a otras empresas sector privado o público que retribuyen mejor que la propia seguridad pública y por lo tanto en un ámbito de progreso y de mejora económica también ha ido a buscar estas empresas que han sabido captar personas que tienen experiencia en dirección, experiencia en el mundo de la seguridad y personal que tiene aquesta esta voluntad para autoformarse a formarse en el mundo universitario. Si esto lo mezclamos, las empresas la calle a buscar a los policías para Desempeñar estas tareas.

Entonces podríamos decir que esta situación ha sido originada por la propia Ley de Seguridad Privada qué es un nivel de exigencia para o con respecto al perfil del director de seguridad es un poquito naif y por esto las empresas aprovechan el conocimiento de los ex miembros de los cuerpos policiales para ocupar este lugar……. .

Sí porque también la seguridad pública es un lugar donde se experimenta mucho donde de alguna manera también tienen experiencia en la dirección de personas. ..... y trabajando en el entorno de amenazas y riesgos desde la seguridad pública También trabajaras en el entorno de los riesgos y amenazas en el mundo privado.

Otro de los motivos podrían ser los contactos, muchas empresas privadas busca en la agenda-.....

Al final la agenda a los 2 años te ha caducado.. Personas que yo conozco del cuerpo de Mossos acaban pasando a segunda actividad: es personal que va rotando mucho. Sí que es verdad que la agenda tiene una validez pero hay que tener presente que caduca muy pronto..

También por otro lado la gente que no viene de la policía dice que no ha tenido ningún tipo de problema para construir está agenda .

Claro porque todos los cuerpos policiales fomentan este tipo de relaciones con el sector privado. Conozco algunas empresas que lo que no quieren directores de seguridad que provengan de la policía. Piensan que tienen una manera de trabajar mucho más jerarquica poco flexible y sometida a la disciplina y no les interesa para su empresa. En cambio también es cierto Que hay gente que viene de la seguridad pública tiene muy arraigada la subordinación porque toda su carrera profesional ha estado empapada de jerarquía y subordinación. Todo tiene sus ventajas y sus inconvenientes. Yo aquí cuando trabajo con personas qué son funcionarios me doy cuenta que su sentido de jerarquia no tiene que ver nada con el policial no es que sea mejor ni peor…. Entiendo que una empresa apueste por persones que tengan arraigado este principio y otras empreses apuesten por la gente que no lo tiene...

3.- Haciendo un repaso al compendio legislativo, y básicamente a la ley del 92, y posteriormente la ley del 2014, ¿cómo valoras las relación entre la Seguridad Pública y Privada?? Cómo. Vaticinas esta relación?

Yo soy un ferviente seguidor de lo público seguramente porque soy el hijo del conserge , y como tal he estudiado en la escuela pública, Y soy una persona a la que la sanidad pública le ha salvado la vida. Sólo puedo defender lo publicó.

Es cierto que muchos gobiernos han maltratado al personal público y no le han pagado de la manera que lo merecía y que las responsabilidades que les dan no están de acuerdo a su sueldo. Yo he tenido la sensación que ha habido como un abuso en este sentido. Por lo tanto, lo que se ha ido haciendo ante la imposibilidad de atender de partidas presupuestarias a la seguridad es que se han ido privatizando diferentes ámbitos . Y creo que esta va a ser la tendencia de futuro y creo que la seguridad privada seguirá cogiendo espacio o espacios de la seguridad pública y cada vez más porque veo que los gobiernos se fijan en una idea y es que la seguridad es un gasto y un coste. Y si esto es así esto seguro que la seguridad privada irá avanzando si se interpretará como una inversión, igual que en la sanidad. Si hubiese este cambio de paradigma la seguridad privada no avanzará tanto. Pero yo creo que cada vez más la seguridad pública va dejando espacios a la privada. Llega el paradigma y al punto álgido en el que el 2009: un gobierno socialista porque era así, autoriza a la seguridad privada a ir en defensa de los atuneros españoles. En lugar de autorizar que la seguridad pública vigile el espacio público que es un

barco con bandera pabellón español lo que hace el legislador es decidir que tiene que ser la seguridad privada la que vaya abordo de los barcos y aviones españoles cosa que indica un poco que los gobiernos apuestan por ceder estos espacios a la soledad privada. Por otro lado, debido al mercado del mundo internacional, las empresas de seguridad privada inglesas americanas, alemanas son las que están dando protección y seguridad a los intereses e ingleses americanos y alemanes en el extranjero. Quiero creer que lo mismo harán las empresas españolas con los intereses del país a MAli, Mauritania, …. a donde se envían estas empresas a proteger los intereses de las empresas españolas, y cada vez más la seguridad privada va avanzando y cogiendo espacio a la seguridad pública. Es cierto que la ley del 2014 se parte del principio de complementariedad pero la complementariedad que interpreta el funcionario de policía sobre la seguridad privada es que tiene que hacer lo que mande y ordene el de la seguridad pública y entonces no le deja esta capacidad creativa o inventiva por lo tanto usted tiene que vigilar Dentro del edificio y de aquí no sale. Esto lo que significa es que de que se habla del principio de complementariedad pero al no entender que el vigilante de seguridad para ayudar a prevenir el hurto en edificios como por ejemplo en el edificio del Palau Güell, el Parque Güell, donde se crean enormes colas, .. y el vigilante de seguridad tiene prohibido salir a la calle y vigilar estas colas. Usted no puede salir a la calle. La cola es una función de la seguridad pública. Pero la seguridad pública no va a vigilar la cola de los Museos y de los cines y los hurteros lo saben, por lo tanto, los delitos de hurto que es uno de los números uno que tenemos aquí, la seguridad privada no puede participar en la ayuda porque se ha decidido sobre una fórmula extraña de que no pueda salir a la calle para vigilar la cola de la gente que tiene que entrar a su casa… Y al mismo tiempo hemos dicho Que las cámaras de seguridad privada no pueden grabar en la vía pública por lo tanto le estamos dando todas las herramientas a los delincuentes para que hagan su trabajo …

Hemos dicho que la relación qué es una relación de complementariedad pero vemos que yo complemento a la pública pero la pública no me complementa me entonces al final es una cuestión de intereses.

Cuando hemos dicho que la seguridad privada tiene la protección del artículo 35 que la equipara al funcionario público y por lo tanto se comete una agresión hacia la el personal de seguridad privada que está bajo las órdenes e indicaciones del personal de seguridad pública,, …… Claro cómo interpreto bajo las órdenes o indicaciones de la seguridad pública, quiere decir que tiene

que estar la seguridad pública al lado con la autorización que yo le pido a la DGAS y ya es suficiente porque la DGAS ya sabe, con la autorización que le pido que ya estoy en la vía pública vigilando una cosa que tenga un valor muy alto y que esté en la vía pública, ...o los que están haciendo la vigilancia en los medios de transporte, y que son empresas privadas que es una tarea que antes hacía la seguridad pública…. Y ahora hace la seguridad privada pero ahora no está a la seguridad pública para dar apoyo o para proteger a la seguridad privada.

Creo que al final lo que ha pasado es que el legislador ha querido dar una fórmula para que los sindicatos de las empresas de seguridad privada estén tranquilos pero que a la hora de ponerlo en práctica veremos como los tribunales interpretan la condición de agente de la autoridad precisamente para que no tenga el principio de la veracidad de los testimonios. Entonces si no se le puede dar este principio de veracidad al vigilante de seguridad porque así lo dice el legislador, y se le restringe esta equiparación en el momento que sea víctima de una agresión y que por tanto la pena para el autor sea más alta Cómo puedes saber el autor que la pena que tiene la agresión es más alta porque este vigilante está bajo las ordenes de un agente de la autoridad... me parece que todo esto se ha liado mucho y supone también una indefensión para el propio agresor porque él no sabrá a qué pena se expone porque no sabrás si estoy vigilante es agente de la autoridad o no lo cual provoca una indefensión que yo quiero creer que los tribunales aplique el principio de in dubito pro reo.

En el tema de la vigilancia de la seguridad privada subida a los barcos creo que también responde a un aspecto de la crisis en la que a lo mejor la parte pública no puede asumir este coste y también sobre ya se está viendo Estados Unidos con los con los Black Waters que son auténticos mercenarios y lo que se busca precisamente es dirimir un poco las responsabilidades de las atrocidades que pueden hacer con lo cual aquí yo veo unos motivos económicos porque la arcas públicas no llegan a tanto y también para dirimir estas responsabilidades. No es lo mismo que un mercenario mate a unos atacantes que lo haga el Estado.

Si te volvería a replicar y te diría que en aplicación de las normas de la Guerra, los estados y los ejércitos tienen la obligación de cumplir la ética militar. En el caso de los ataques, sí el Canarias que es la fragata que está protegiendo los barcos puede hacer uso de las armas de fuego con material bélico, deberá pedir permiso a Madrid, Madrid a Bruselas y Tendrá que ser OTAN quién autoriza el uso de las armas. Efectivamente si lo hace un gigante de seguridad no

tendrá que hacer uso de este circuito y podrá hacer uso de la fuerza en ese mismo momento bajo el supósito de legítima defensa. . Cómo decías tú, que si era una cuestión de recursos o dinero este Vigilante de Seguridad Privada que llega y tiene que hacer frente a un ataque mediante el uso de de las armas,lo que pasará es que es que a este vigilante se le habrán restringido sus derechos,...Lo que habremos hecho es habremos embarcado a un vigilante y al cabo de un año haya vuelto al punto de partida.. ¿cuántas horas habrá hecho este vigilante ?? Su régimen laboral dice que cada 8 horas tiene que descansar y tiene que haber un segundo y un tercero para hacer un relevo. La seguridad pública no podría comportar esto, necesitarías 5 personas por turno y cada 3 o 6 meses se relevase a la plantilla… En cambio en la seguridad privada no se respetan estos derechos y por lo tanto sí que sale más barato. No se tienen en cuenta ni las normas de la guerra ni los derechos de los trabajadores. Creo que esto es una cuestión yo diría que de ingeniería y de química de cómo organizamos para que el sector privado pueda aparcar y utilizar armas de guerra porque también se ha tenido que cambiar el Reglamento de Armas y el Estatuto de los Trabajadores, y la Ley de Seguridad Privada. Se tuvo que cambiar todo para hacer esta ingenieria, para permitir que la seguridad privada vaya en los barcos. Por esto yo creo que en un futuro la seguridad privada va ganando terreno la seguridad pública.

4.- Eres el DS de la Diputació. ¿Cuál es tu día a día?

Yo ahora, básicamente a las 8 cada día recibo los partes y llamadas de todos los vigilantes de seguridad de la Diputación y me dicen si han tenido alguna novedad en alguno de los espacios de la Diputación. Además todos los organismos autónomos de la Diputación que actualmente tenemos 114 oficinas encargadas de la gestión y cobro de tributos y multas de los ciudadanos, también hemos tenido alguna que otra amenaza a los empleados ,.... o algunos museos que dependen de nosotros.

Cada día me llega entonces la información de estos vigilantes de seguridad que dan servicio de cobertura a todos estos edificios…

Por lo tanto si se ha producido Un hecho relevante se intenta gestionar.

Por otro lado lo que se hace a continuación es todo el asesoramiento de alcaldes y municipios y entidades que dependen de la Diputación. En este momento estamos haciendo el Plan Director de Seguridad del Instituto del Teatro. A intentar hacer ver a los responsables políticos que necesitan unas herramientas que les permitan y que les ayuden a dirigir la seguridad en sus

espacios. Sí ha de cambiar esta idea de que a esta hora ellos pensaban que la seguridad la puede hacer cualquiera, les tenemos que hacer ver que sí que lo puede hacer cualquiera pero si está todo y todo preparado estructurado y de acuerdo a la normativa.

Por otro lado también tenemos toda una serie de incidentes en los edificios en los que se estropean cámaras, alarmes, sensores y que por lo tanto se ha de gestionar los diferentes técnicos para ver lo que ha pasado, o dar cumplimiento a mejoras de seguridad porque hemos tenido unas nuevas amenazas en nuestros recintos como puede ser la instalación que estamos haciendo del sistema de seguridad ahora en Canet de Mar la Escola del teixit o en Terrassa en el museo de diseño.

Por lo tanto el día a día tiene una parte de urgencia inmediata de lo que ha pasado, tiene una parte de supervisión de lo que se está haciendo en cuanto a la planificación y tiene una parte de control y supervisión de los 150 vigilantes.

Cuáles son las amenazas recurrentes a las que tienes que hacer frente y qué medidas utilizas para tal efecto?

En estos momentos la amenaza que tiene el país que así lo dice la seguridad pública es el terrorismo. Ante el terrorismo y la alerta 4 lo que hay que hacer es plantear el cambio de criterio en nuestros vigilantes ante la gran proliferación de personas. En Barcelona, muchas de las personas que salieron corriendo después de los atentados de la Rambla se fueron a refugiar en instalaciones nuestras y nos dimos cuenta que no necesitamos cambiar las medidas de seguridad por si el otro està, por si se hubiese colado en nuestras instalaciones. Eso también ha puesto de manifiesto que se tiene que dotar en determinados servicios a los vigilantes de seguridad con armas. Por otro lado sí la seguridad pública ha decidido que a sus trabajadores los protege con unos chalecos antibalas y anticorte lo que tenemos que hacer es estudiar cómo puedo cambiar las condiciones laborales para que puedan tener este chaleco antibalas cuándo trabajen conmigo para que cuando se pongan al lado, uno al lado del otro tengan las mismas medidas de seguridad… pone de manifiesto que hay que cambiar los contratos del personal. Con lo que también se ha de tener en cuenta la nueva Ley de contratación y cómo puedes cumplir con esta normativa siempre cuando se ajuste al servicio que tú quieras dar que el vigilante tenga un chaleco etcétera.

Después al mismo tiempo que das respuesta a esta amenaza ver cómo estás al día con las nuevas tecnologías y como estas nuevas tecnologías te pueden producir un ahorro en el gasto o un

ahorro de las medidas o un incremento la Seguridad, si utilizo cámaras térmicas, drones, si cambio el sistema analógico al sistema digital,.... ver como utilizo esta tecnología para que sea útil. ¿En que sentido? Pues adecuándonos a lo que nuestros trabajadores y personas que protegemos..... los 4000 funcionarios también van cambiando. Hasta hace 4 días nadie venía en bicicleta al trabajo y ahora muchos vienen a trabajar en bicicleta, por lo tanto, necesitamos tener parking de bicicletas y elementos de seguridad para las bicicletas en los parkings. ¿Cuál es el mejor sistema de seguridad para asegurar una bicicleta? Pues tendremos que estudiar lo que hay en el mercado. Lo mismo con las tarjetas y tecnologías para identificar accesos. Ahora las hemos tenido que cambiar porque parece que no cumplen con las medidas de seguridad y el mercado nos ofrece otra tecnología. ¿Cuáles son entonces aquellas tarjetas que no se puedan falsificar y le permitan al trabajador abrir determinadas puertas y qué pueda hacer fotocopias y que también pueda dejar la bicicleta y aparcarla en un establecimiento y por lo tanto ver que hay en el mercado como nuevo elemento de seguridad que me permitan a mí avanzar?

Y finalmente, también a ir a parte de lo que sería el patrimonio y la protección al patrimonio hurto estafa robo fuerza etcétera.

Después todo aquello que tengan a ver con la ciberseguridad y la seguridad de aquí dentro. Nosotros coparticipamos y colaboramos con la ciberseguridad desde el punto de vista que somos conocedores de los elementos de seguridad que hacen falta ahí donde estén las CPU's, los sistemas informáticos que tenemos que proteger, digamos que el cerebro de la bestia de la Diputación y por lo tanto la protección de estos datos. ¿Cuáles son las medidas entonces que debemos seguir para proteger la información de nuestros usuarios y contribuyentes? Por lo tanto quiere decir que en Ciberseguridad tienes que entrar a trabajar en ciberseguridad codo a codo con los ingenieros informáticos para que tengan elementos de seguridad en los accesos y determinar qué personas pueden y no pueden entrar . Sólo el director de seguridad puede decidir en una empresa, en aplicación del artículo 36 quién puede y no puede acceder en un espacio determinado. Y por otro lado, como nosotros tenemos muchos bienes, y son susceptibles de ser atacados, y nos los han atacado...

Por otro lado también tengo que saber lo que pasa en las redes sociales. Las amenazas que antes eran físicas ahora también pueden ser digitales afectan al prestigio de la entidad. La reputación digital es una cosa que también controlamos al os desde aquí conjuntamente con el personal de comunicación. controlamos todas estas amenazas contra la Presidenta, diputados, contra los

altos cargos. Actualmente hay denuncias interpuestas porque al nuestro entender hay usuarios de las redes sociales que se extralimitan en el ejercicio de su derecho a la libertad de expresión… Nosotros a la seguridad pública les facilitamos los certificados de los días y ahora en los que han salido estas amenazas… estas amenazas pueden ser amenazas digitales contra la reputación, contra el patrimonio o contra trabajadores que sufren acoso y persecución y nosotros ayudamos a estas personas que se sienten víctimas de un delito y las asesoramos para que vayan a denunciar si creemos que son víctimas de un delito.

Cómo estructuras el departamento de seguridad???

Yo llego aquí hace 3 años donde el Departamento de Seguridad pertenecía al área de logística, que se dedicaba a elementos o aspectos como la limpieza y también a la seguridad. Cuando ya llevo aquí lo separo y damos independencia y actualmente dependemos de Presidencia. Cuando llegué aquí solo había una una unidad técnica y una unidad cooperativa que se dedicaban básicamente hacer contratos de tecnología o contratos de vigilancia. Primero lo que hice es un plan estratégico de seguridad que fue aprobado por la Presidenta y después de este Plan estratégico de Seguridad cuelgan los diferentes planes directores de seguridad de los recintos o de lo que serían los organismos autónomos, los organismos de gestión tributaria que tienen sus propios planes de seguridad.

Como la gente que había aquí no tenía suficiente formación. Se firman convenios con la Universidad para que a estas personas reciban la formación en seguridad. Después hemos ido contratando técnicos e ingenieros. Actualmente tenemos tres ingenieros en el departamento. El resto de personas que están con ellos son técnicos que acompañan a las empresas instaladoras para ver cómo hacen o dejan de hacer las instalaciones. Por lo tanto, ahora de esta Unidad Técnica o operativa la hemos pasado a una unidad técnica, a una unidad administrativa más una unidad reputacional y a otra unidad de ayuda y análisis en materia de seguridad a los municipios.

5.- **Estamos en la sociedad que hacemos un uso muy exhaustivo de la tecnología cada vez más pero no hay una cultura de seguridad de lo que hay detrás de todo esto. Esto pasa en todos los niveles no sólo a nivel de usuario sino también de gerencia y hasta nivel de los juzgados que no quieren saber nada de tecnología. Entonces yo relaciono esto y se produce una cosa muy curiosa en temas de ciberseguridad y es que la ciberseguridad muchas veces o en la**

mayoría de las veces no se lleva desde el departamento de seguridad sino desde departamento los sistemas de información y esto a mi modo de entender es como si yo mismo me hago una auditoría de mi empresa, saldrá bien porque me interesa que salga bien. Yo esto lo relaciono con el desconocimiento que hay en los departamentos de seguridad de la propia ciberseguridad entonces me gustaría preguntarle desde dónde se gestiona la ciberseguridad en la Diputación y como cree usted que tendría que ser este modelo.

Yo coincido plenamente contigo y creo que la ciberseguridad debe llevarse desde el Departamento de Seguridad. Ahora bien, cuando llegué aquí hablé con la Presidenta y con el responsable de sistemas y no estaba de acuerdo con mi planteamiento. La Presidenta tomó una decisión salomónica y en el decreto de seguridad la ciberseguridad depende de los dos depende de sistemas y del de seguridad. y depende de los dos porque Al final la responsable final de la ciberseguridad es ella. Todos los ingenieros que trabajan en ciberseguridad dependen orgánicamente del departamento de sistemas y funcionalmente del Departamento de Seguridad.

Cuando Guardia Civil Mossos o Policía Nacional nos alerta me avisan a mí y automáticamente informo a ellos si hay un virus o cualquier otra cosa. También esto pasa a la inversa cuando recibimos muchísimos ataques soy yo quien aviso a las agencias de ciberseguridad que está pasando todo esto.

Yo coincido contigo pero no sólo por esto sino también porque el responsable de ciberseguridad como es el responsable de los sistemas está preocupado en su día a día de que los servidores funcionen de cuando toques al botón funcione y entonces el mismo me decía que le cuesta mucho decir a la gente que cambie el password cada tres meses. Yo le dije no no.... si tú no le tienes que decir nada es la propia máquina automáticamente lo tiene que hacer y ya está. A él según me decía le costaba imponer esto y yo le decía a mí no me cuesta en absoluto por lo tanto di que lo digo yo y a partir de aquí será así. Cuándo ahora pongamos las tarjetas digitales él decía estoy seguro y convencido de qué la tarjeta se la pasará el gerente a la secretaria y será la Secretaría que el enchufe que entre… y yo le dije que si somos capaces de ver esto porque hay una persona que tenga dos IP'S en uso ya iré yo y le diré que esto no se puede hacer. Claro es muy difícil cambiar esta línea yo creo que en los próximos años irá cambiando así y la tendencia será esta. lo que no puede hacer es entrar como un elefante en una cacharrería.

Para mí lo más preocupante es cuando vas a los ayuntamientos a asesorar a los alcaldes y a explicarles todo esto como tú bien has dicho no hay cultura de seguridad ni conciencia de seguridad.

Sí nosotros damos servicio a todos los municipios, servicios informáticos y les gestionamos el cobro de los tributos mediante el uso de nuestro sistema informático nosotros hemos puesto elementos de seguridad que cuando ellos se dirigen hacia mí tienen que pasar por un filtro por lo tanto me aseguro que quien entra aquí tiene que pasar por determinados filtro y todo lo que me entra es limpio.

Este año hemos conseguido una partida presupuestaria para hacer una prueba piloto con 20 ayuntamientos. Decidimos hacer un plan piloto que consistía en implantar una célula para poder monitorizar el tránsito las entradas y salidas de estos ayuntamientos desde la persona que se descarga películas porno por tipo de películas y nos dimos cuenta que había millones de bytes que entran y salen evidentemente lo hicimos con el consentimiento de los ayuntamientos lo que nos encontramos cuando llegamos es que los antivirus, las licencias de microsoft y los firewalls eran piratas y cuando hablas con el informático lo primero que te dice es que se acabó el presupuesto y se acabaron las licencias y cuando yo pedí dinero para comprar las licencias no llegaba el dinero... Entonces, hicimos un paso hacia atrás y de cara al 2019 para que los ayuntamientos que no lo tuvieran pudieron actualizar las licencias Windows, …. cuando ya las tengamos legales podremos hacer otras cosas, le podemos conectar una célula para monitorizar el tráfico etcétera etcétera y poder, … establecer las políticas de contraseñas copias de seguridad.

6.- Hablemos ahora de Inteligencia. Qué es para ti y cuál es su valor añadido??

Nosotros lo que intentamos hacer es de toda la información que generamos la trabajamos y vemos cómo la convertimos en un hipotético riesgo i amenaza para nuestros diputados, políticos y gestores. Recogemos toda la información que nos producen los 4000 funcionarios más la que nos ofrece los servicios que préstamos, y prensa etcétera etcétera más fuentes internas de trabajadores que nos dicen lo que ven y lo que han dejado de ver… Todo esto llega el departamento formado por 2 personas, aunque yo quería que fueran más, de las cuales una se ocupa básicamente todo el día de la red porque hoy en día en la red donde hay millones de información . Recuerdo que entradas en el Twitter con información referente a una persona de aquí dentro había 2600 y 1400 más de 1000 en el Facebook . Aunque tú metas una araña y te

busque y te encuentre información al final tienes un problema para seleccionar qué información es útil o cuál será una amenaza real o no. Por lo tanto, esta persona que debería hacer análisis prácticamente se pasa las 8 horas del día analizando la información que heredan las redes sociales.

Después de toda la información que va llegando la otra persona es la que se encarga de analizar a partir de la agenda de la Presidenta, a partir de la agenda de los Diputados, y a partir de la agenda de los alcaldes en los actos públicos que hacen lo qué puede aparecer en la red en cuanto a manifestaciones contra sus actos o su persona. Por lo tanto hay una mezcla entre la información que se obtiene por la vía pública dado la Ley de Transparencia y otra información de carácter más interno.

Como aquí también tenemos la escolta del presidente que es un caporal y tres Mossos cuando tenemos sospechas de una amenaza o algo que se complica bueno pues lo hacemos entrar a las unidades de información del cuerpo policial que corresponda.

INFORMACIÓN QUE NO PUEDE SALIR HACERSE PÚBLICA, ….

Nosotros cuando tenemos un acto en el cual va un diputado o un regidor y vemos que el nivel de comentarios y nivel de amenazas a raíz de los comentarios la raíz es considerable lo hacemos llegar a las fuerzas y cosas de seguridad para decirles que tal día tendrá lugar el acto y que hemos detectado esta tipo de información.

Tengo una teoría, y es que a través de la inteligencia, podemos obtener información que hasta su llegada, la de la inteligencia, estaba sólo en manos de las FCSE. Se ha dado el caso en el que has recibido información mediante inteligencia mucho antes de recibirla por la vía tradicional (FCSE). En una sociedad denomidada la sociedad de la información, donde quien tiene la información tiene el poder, si la parte privada dispone de más información porque tiene más medios y por lo tanto tiene poder, ¿no crees que la relación entre la seguridad pública y privada se verá afectada y situará a la seguridad privada en una situación de ventaja, más allá de la complementariedad que determina la ley?, ¿ Crees que esta casuística va a cambiar la relación, no de Iure sinó de facto, entre la seguridad privada y la seguridad pública?

Si es así lo veo igual que tú.

De todas maneras nosotros somos una admistracción pública Por lo tanto lo que nosotros tenemos y lo que analizamos está relacionado con la seguridad pública pero evidentemente podríamos privatizarlo, podríamos coger un DOLAITE y encargarles está faena. Yo, en principio,

no quiero hacerlo porque soy partidario de lo publicó pero también es cierto que hay ciertos casos como por ejemplo el del Oleguer y de la Selva y su empresa que son una gente muy potente. Y entre tener una persona que está aprendiendo a tener una empresa comopuede ser onbranding o Oleguer trabajando allá ... dices hombre es que esta gente lo hace muy bien. Entonces lo ideal sería que nosotros ese lo publicó lo hiciéramos también como ellos pero no tenemos ni recursos ni los medios ni el sistema.

Y a veces nosotros nos ponemos piedras en los zapatos. ¿Porque Oleguer lo puede hacer mejor que yo? porque es mucho mejor que yo y ya està, y porque además tiene una capacidad innata que yo no tengo. Y después hay otro elemento y es que es que yo tengo que trabajar con servidores y buscadores que sean residentes en la Unión Europea y ellos no. É puede trabajar con servidores situados en San Francisco o Los Ángeles y yo no. Esto me condiciona y me limita porque su servidor y buscador desde Los Ángeles es mucho más potente que los que yo puedo hacer servir aquí. O sus herramientas estadísticas son mucho más potentes a las que yo tengo acceso. En definitiva, yo no puedo comprar esas licencias porque no son residentes en la Unión Europea y esto yo no tengo manera de luchar. Somos nosotros que nos hemos limitado y tenemos que esperar que una empresa catalana francesa o lo que sea Europea desarrolle herramientas tan buenas como las que hacíamos referencia.

7.- Imagínate que eres el director de RRHH de una gran empresa y el CO te encarga contratar un DS. ¿Qué buscarías en en DS?

Buscaría un perfil de persona que sobre todo supiese escuchar y que tuviéra empatía, que supiera escuchar a los trabajadores porque básicamente la gente dentro es la que más conoce cuáles son las principales amenazas. La típica persona que es callada que no habla pero cuando tú te acercas a hablar con ella te das cuenta de que es la persona que más sabe de su entorno. Y también de alguna manera el vigilante que está en la puerta lo sabe todo de todo el mundo cómo viene cuando viene con qué coche viene…

Por lo tanto lo primero que le pediría es que supiese escuchar

La segunda es que tuviera una mentalidad analítica qué supiese determinar qué datos relevantes son los que determinan una amenaza o un peligro.

También le pediría que tuviera una gran capacidad de superar la frustración porque el director de seguridad siempre necesita más dinero más recursos y siempre le recortan presupuesto y gente. Tiene que de tener un espíritu constante, con un sentido de la responsabilidad muy alto

con una capacidad de sacrificio y esfuerzo. Que no fuese una persona que se planteaba entrar a las 8 y salir a las 5 porque esto no es un trabajo estable en este sentido no puedes saber tu horario, porque la cantidad de cosas que te pueden pasar son tan inversemblantes que no puedes planificar…..

Al final el director de seguridad también tiene que ser una persona con suerte, que sea optimista. Porque en seguridad necesitas una dosis de suerte a la hora de hacer las cosas y si puede ser con una sonrisa mi mejor. En definitiva, una persona que se aleje al típico director de Seguridad con el traje gafas de sol con muchas horas de gimnasio… a mí esto no me hace falta. al final me inclino por una persona que sepa sonreír que sepa escuchar que sepa agradecer a sus trabajadores cuando hace las cosas bien pero también que sepa reñir cuando no lo hacen pero también que tenga un poquito de suerte.

6.- Al mismo tiempo que esta persona que esté de director de Seguridad tiene que escuchar (y esto que le voy a decir no está ninguna ley) creo que también una de sus funciones es infundir la cultura de seguridad.

Yo lo que te lo que estoy intentando hacer aquí es un cambio de paradigma en cuanto a la seguridad y hacer ver a la gente que la seguridad no es un gasto sino una inversión. Pero si tú esto lo haces diciendo la gente infundiendoles el miedo diciendo que va a venir el lobo va a venir el lobo y resulta que cuando viene el lobo le dices que ya se lo habías dicho esto no te lleva a nada. Esto no te va a conseguir una mayor partida presupuestaria per seguridad ni un cambio de criterio.

Cuando entras al Consejo de Dirección de la Diputación que son veintitantas personas, Directores y Gerentes y gestores, si tú les hablas de tú a tú diciéndoles como tú les puedes ayudar a ellos y como ellos te pueden ayudar a ti, consigues un cambio de cultura. Desde que hago esto, desde que bajo a las reuniones y les pido que me ayuden en algún campo, ellos también me piden que yo les ayude a ellos.

Ellos ya empiezan a pedirme a mí cosas de seguridad cuándo van a hacer sus proyectos.

Por lo tanto creo que el éxito está en que sepas escuchar no nada más a los de abajo sino también a los de arriba. A veces tu sola presencia hace que cuando te ven ellos empiecen inconscientemente a cambiar su paradigma Y para eso no hace falta que sea infundiendo el miedo. Al final la seguridad requiere la corresponsabilidad de todos y la responsabilidad de

todos, de los de arriba y de los de abajo y para esto el Director de seguridad debe ser capaz de escuchar y convencer sin imponer su criterio.

11.8 Entrevista Eduard Zamora

FICHA TÉCNICA	
Descripción	Entrevista a Eduard Zamora, exdirector de seguridad Banc de Sabadell
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector.
Fecha	26 de -marzo del 2018
Lugar	Dependencias Banco Sabadell (Sabadell)
Observaciones	

1.- Eduard, no nos conocemos … la primera pregunta me lleva a saber más de ti. Cuál ha sido tu trayectoria profesional hasta llegar a estar donde estás. ¿Cuál ha sido el recorrido?

Es una larga historia porque tengo 59 Años y llevo trabajando desde los 14 con lo cual sólo me centraré en la parte relativa a la seguridad. Antes de entrar a trabajar en el banco trabajaba en la Policía Local de Sabadell, era sargento y gestionaba los servicios del cuerpo, la secretaria, la plana mayor, después los recursos de depósito de vehículos, atestados etcétera.
Cuando estaba allí tenía ciertas discrepancias con el regidor que llevaba la Policía Municipal en aquel momento entonces me salió una oportunidad en el banco porque en aquella época en el banco había dos personas en el departamento de seguridad y una de ellas se iba. Mi mujer que trabajaba en aquellos momentos en recursos humanos del banco me dijo: buscan un candidato que se ajustaba mucho a tu perfil y cómo que tú no estás muy contento porque no te dejan hacer todo lo que quieres hacer en la prefectura de la Policía Municipal de Sabadell…. porque yo hace más de 30 años que quería implementar criterios de gestión privada dentro de la Policía Municipal de Sabadell. Esto que ahora se está haciendo en Mossos y policías locales en otros sitios pues hace 30 y pico años era un poco extraño. Todo era siempre no no tú estás loco tú

estás loco no no no y al final me cansé y pensé: voy a buscar trabajo. Salió esta oportunidad en paralelo con otra que era la del hospital de Sabadell y al final opté por estar aquí te estoy hablando de hace 29 años. El día que hacía 6 años en la Policía Local y me acuerdo porque era el segundo trienio, no lo acabé cobrando porque al día siguiente entre aquí.

Aquí comencé como puedes imaginarte…. éramos dos, era el nuevo en llegar y comencé muy de base y al final el apartamento se hizo más grande y poco a poco fui cogiendo nuevas funciones. Finalmente, y esto es una anécdota, la persona que se iba no se fue. Cuando ya estaba todo atado dijo que no se iba porque tuvo un malentendido con el suelo del sitio donde iba porque iba al hospital de Sabadell y como no se entendieron en el sueldo o él lo entendió mal o lo dijeron mal… Total que dijo que no marchaba. Claro, entonces había un problema porque yo entraba porque se iba uno de los dos y uno de los dos no se va, y ahora ¿qué? Mira sabes que te quedas porque igual esta persona de aquí a poco esta persona seguirá buscando y se marchará y nos ha parecido que por tu perfil y por tu experiencia y por tu formación y por tu forma de ser nos puedes ayudar…. y me quedé. En aquel momento el banco era un banco pequeño con 2 personas íbamos sobrados de faena, no hacía falta más gente y me tuve que empezar a espabilar para intentar ganar funciones dentro de la casa y una de las primeras que conseguí fue convencer al banco de que se montara era toda la parte de, …. porque yo soy abogado penalista y les propuse llevar aspectos de gestión penal, Ejercer la acusación particular contra los atracadores, Estafadores …. y comencé trabajando dentro como técnico de seguridad compaginando estas tareas de técnico de seguridad con análisis de riesgos y otros estudios que hacía y trabajando ejerciendo como abogado la acusación particular. Estuve unos cuantos años pateándome todos los juzgados de España acusando a todos los atracadores, falsificadores, ... en aquella época había muchos atracadores. Hoy en día todo se ha decantado hacia el fraude. En aquella época era más típico el robo violento de toda la vida. En este impás surgió la oportunidad de crear la Dirección de Prevención de Riesgos Laborales y también la empecé a organizar dentro de seguridad. En este impás el banco decide que en lugar de ser un colaborador de la Dirección de Seguridad que pase a ser yo el director de Seguridad y así he estado alrededor de 20 años hasta enero del 2017 que salgo de la Dirección de Seguridad por qué se considera que hace falta, que después de tantos años con una misma función, convienen aires nuevos como en su día me pasó a mí cuando me ofrecieron la Dirección de Seguridad del grupo. Ahora llevo más de un año trabajando en un proyecto de creación de la nueva dirección de continuidad

de negocio del grupo y ahora desde la semana pasada que he acabado este proyecto estoy colaborando con la reordenación de la dirección nueva de gestión de proveedores porque amplía competencias y supongo que será otro año de colaboración con este proyecto. Mientras que continuidad de negocio es algo cercano a la seguridad porque al final el taranná es muy similar porque hay incidencias más o menos graves y tienes que reaccionar para que no perjudique a la actividad del banco. En seguridad hay un componente muy similar ahora sí que sí que después de tantos años ha habido un cambio de chip importante. Esto significa que he estado trabajando de los de 34 años en seguridad entre la parte pública y la parte privada. Ha sido una experiencia buena positiva y muy importante para mí para poder crecer como persona y como profesional.

2.- No es ningún misterio ni secreto que los puestos de DS los están ocupando en un gran porcentaje ex-miembros de cuerpos de fuerzas y cuerpos de seguridad del Estado. ¿A qué crees que se debe?

Yo en el fondo no dejo de venir de un cuerpo policial pero evidentemente no creo que tenga nada que ver a lo que tú te refieres. Porque yo no entré de un cuerpo policial en el cual tú renuncias a tu actividad policial y evidentemente algunos funcionarios policiales cómo Guardia Civil y Policía Nacional tienen sus famosas excedencias y segundas actividades que te permiten ganar una parte importante de tu sueldo dedicándote a trabajar en otros ámbitos entre ellos …mucha gente sobre todo altos mandos trabajan mucho en temas de su vida privada. Y aquí es fácil que las grandes corporaciones si te fijas ... Una de las cosas que me sorprendió cuando entre aquí me dijeron que no querían un policía sino grandes expertos en seguridad privada y no pública y me dijeron que les tendría que convencer de cogerme a pesar de que yo fuera un policía.

Esta tendencia yo creo que ha cambiado porque han cambiado los perfiles y las empresas y la rutina de la gran mayoría de grandes empresas sobre todo las del Ibex como es nuestro caso y sí que se tiende a que gran parte de ellas a qué altos mandos policiales entran a trabajar y la banca es un gran ejemplo de que la gran mayoría de bancos tienen como directores de seguridad de un ex cargo policial de la Guardia Civil y sobre todo básicamente del Cuerpo Nacional de Policía.

Nosotros no; nosotros seguimos, yo … podemos decir que no era este perfil y la persona que ocupa esta función en el grupo evidentemente no lo es porque no viene ni tan solo lo del mundo

de la seguridad. Viene de otros ámbitos, pero al final como el equipo ya está creado lo que necesita es un gestor. Necesitas un perfil de personas que dominan mucho la materia en empresas pequeñas pero las grandes empresas, y te hablo de lo que es nuestro modelo que evidentemente si te vas a otros bancos verás que es diferente y te acabo de decir que casi todos ellos tienen altos cargos policiales. Hay alguna excepción en la que se piensa que no hace falta porque el equipo de técnicos expertos en su materia seguridad física electrónica fraude análisis de riesgos Inteligencia Criminal y todas estas cosas son bastante buenos y que lo que hace falta es una persona que los coordine y este ha sido el criterio del Banco para encontrar la persona que ostenta esta función. es la persona que viene internamente de la casa del mundo bancario que no tiene nada que ver con la seguridad.

¿Cuál crees que es si lo hay el valor añadido?

Mira yo he estado 9 años, 6 años presidente Y 3 VICE PRESIDENTE de la Asociación De directivos de seguridad integral; una de las 3 más importantes por volumen de socios y de actividades … casi me atrevería a decir que es la primera que tiene sede en Barcelona pero que tiene ámbito nacional, en la cual yo desde la posición de intentar de reforzar al máximo la función y la funcionalidad de los directores de seguridad una de las cosas que siempre había comentado no quiero decir criticar si no comentar era el exceso de recurrir a la cantera de altos cargos policiales para ostentar la Dirección de Seguridad tanto de grande empresas como de empresas no tan grandes. ¿El valor añadido? evidentemente los contactos y el trabajar cada día con seguridad, evidentemente la mentalidad de haber de prever que no me pasen cosas en el Ayuntamiento, en la administración o en la empresa privada. Este vivir el día a día de la seguridad y sobre todo los contactos que los tienen mejor que otros que puedan comenzar a salir de las escuelas ahora ya como es tu caso de las universidades pero si los que están comenzando con estos temas consiguen el nivel de complicidad que es una palabra que me gusta mucho decir que siempre la he dicho mucho en las universidades donde he hecho clase a personas que tienen estas inquietudes, una parte importante de tu sitio o lugar de trabajo será ganarte la complicidad no sólo de la administración sino también de otras empresas del sector o de fuera del sector .Cuando tú tengas está complicidad Ganada tendrás muchas puertas abiertas, conocerás muchas incidencias casuística y soluciones que los compañeros de las agencias de seguridad y los policías y los que hagan falta no tendrán ningún problema en compartir contigo pero tienes que ganarte esta complicidad. Y mientras no te la ganas evidentemente que algunas empresas

pueden pensar que los altos cargos policiales ya tienen ganada está complicidad como mínimo de la policía y también de otras entidades con las que seguramente ya han trabajado. Pero yo no soy muy partidario de que la mayoría de lugares de trabajo las ocupen ex policías.

Aquí hay dos visiones. en una entrevista con un alto mando que ahora es director de seguridad no niega la importancia de los contactos, pero me dice que está agenda dura 2 años.

En este sentido hay un componente de relación importante en la función de un director de seguridad de una gran corporación y aunque no sea tan grande también. Hay un componente relacional importante qué has de cuidarlo, evidentemente has de trabajar y todo el mundo puede pensar que ahora lo que quiero decir o lo que quiero dejar intuir es que te has dedicar a hacer relaciones …. es, pero esto no es así. Lo que tienes que hacer es no descuidar las. no me atrevo a decirte un porcentaje a lo mejor un 25 o 75 25 mantener relaciones o cuidar relaciones y 75 el resto.
Es un aspecto importante que no has de abandonar porque cuando tengas incidencias difícilmente serás tú la primera persona que las sufra y creo que es bueno por esto compartirla con el resto con el resto de compañeros de seguridad del sector. Si tú te ganas esta complicidad tendrás acceso a mucha información y como yo siempre he pensado que no hace falta inventar la rueda porque ya está inventada… a ti te puede gustar más con un radio de titanio y al otro de aluminio, pero la rueda ya está inventada. Entonces el componente racional es importante para poder conocer y recoger y aplicar soluciones qué otros ya están aplicando y si tú tienes esta complicidad tendrás mucho más fácil acceso a conocer y a que la gente comparta contigo de la misma forma que tú hablas de compartir porque esto es en gran medida un QUID PRO QUO.

3.- **Haciendo un repaso al compendio legislativo, y básicamente a la ley del 92, y posteriormente la ley del 2014, en la que en el 92 subordina la privada a la pública i que después la ley del 2014 la sitúa como complementaria, …. Me gustaría que me dijeses como director de seguridad, ¿Cómo ha sido esta relación?**

Mira, la relación siempre ha tenido un componente muy difícil que es la relación con la administración tanto antes como ahora. Cuesta poco escribir, es como un plano que los que son

arquitectos dicen que siempre cabe todo cuando estos sobre el terreno lo aplicas las cosas no quedan tan bien como pueden quedar en un plano y esto es lo mismo las palabras quedan muy bonitas pero las tienes que aplicar entonces evidentemente la diferencia del texto es importantísima antes era de subordinación y ahora es de colaboración pero resulta que si las tienen que aplicar son las mismas mentalidades y las mentalidades cuestan mucho que cambiar mucho más que un texto. La mentalidad de los dirigentes policiales e incluso no hace falta que sean altos mandos sino mandos intermedios que probablemente será con los demás interactúe cuesta mucho que cambie mucho más que el texto de la ley. Al final esta complementariedad sigue siendo bastante subordinada no quiero que parezca peyorativo, pero sigue siendo de escúchame yo soy la policía yo soy la administración y tú eres un administrador y tú te tienes que someter a mis peticiones como yo diga.

Todo está dentro de un orden y dependerá de que es lo que me pidas de cómo me lo pidas porque yo también puedo hablar tranquilamente temas de protección de datos.etc y puedo poner bastantes impedimentos en tu faena de investigación o la que puedes hacer dentro del cuerpo… al final lo importante es esta complementariedad: yo te ayudo, sólo faltaría porque si tú triunfas yo triunfo porque si tú triunfas policialmente los delincuentes estarán condenados y yo me beneficiario. Si tú triunfas policialmente la percepción de que la seguridad pública tiene bastante éxito y la boca a boca entre la delincuencia no será el típico mensaje de decir esto es Hollywood y aquí podemos hacer lo que queramos porque la vigilancia policial es mínima. Cuando más nos ayudemos mejor tú ganasen eficiencia es un win-win. Es cierto también que está costando mucho más de lo que a priori la misma normativa podía pensar que no nada más cambiarlo ya estaría.

Creo que hace falta alguna década y esperamos que sólo sea una que cambien mentalidades que nos demos cuenta que todos estamos en el mismo barco.

Yo siempre le decía la administración: escucha no te equivoques que el más preocupado por proteger la entidad que me paga el sueldo soy yo y no eres tú porque yo me juego el sueldo y tú no y por lo tanto no dudes de que estamos en el mismo barco y todos estamos encaminados hacia la protección de mi empresa y del resto y si yo puedo ayudar a otras entidades mejor que mejor.

Yo siempre había recriminado y sigo recriminando que estamos en el mismo bando los dos luchamos contra la delincuencia, las sanciones no todas no aquellas que se han interpretables

hazlo de manera que siempre no me perjudique porque siempre me perjudica al final pienso que tú te piensas que yo soy el malo.

4.- Eras el DS de la BS. ¿Cuál era tu día a día?

Mira yo diría que un día a día es que no tienes día a día, que no tienes planificación porque lo bueno y lo malo de un trabajo como este es que como tú no dependes de ti mismo si no dependes de lo que los delincuentes hayan pensado que te quieran hacer el fin de semana anterior o la noche anterior o durante el mismo día tú ya puedes planificar tu agenda tú reuniones todo lo que pienses que tengas que hacer ese día de esa semana pero la casuística delictiva del momento y porque no de las necesidades de la alta dirección de cada momento serán las que condicionarán tu agenda. Evidentemente sin perder de vista que tú tienes unos objetivos anuales qué deberías intentar cumplirlos. Que estadísticamente el nivel de protección o de vulneración o de incidencias que cada entidad quiera porque cada entidad fijará el listón allá donde crea conveniente en función de las inversiones que debo hacer para bajar un grado más el listón o mantenerse. Y evidentemente lo que no debemos olvidar es el nivel de seguridad que marca la normativa. Este es negociable todo y que algunas compañías no es nuestro caso pero me consta hablando con otros compañeros que incluso intentan recortar de allá dónde es legalmente obligatorio disponer de un mínimo nivel de seguridad físico o electrónico determinado y lo hace porque siempre se ve y se ha visto como difícil de determinar cuál es el rendimiento de esas inversiones.

¿Qué pasaría si la Dirección de Seguridad ya no funcionaba? pues a lo mejor nada.

¿Qué pasaría si la seguridad pública o la policía un día no funciona? bueno si lo haces público y notorio seguro que pasarían cosas, pero si no se hace público igual no pasa nada, hasta lo mejor es mucho mejor estadísticamente que los mismos días de otros años anteriores. Pero evidentemente cuando se hace público y notorio que la seguridad no está vigente, que la policía no está trabajando seguramente el perjuicio será mucho más grande.

¿Cuáles son las amenazas recurrentes a las que tienes que hacer frente y qué medidas utilizas para tal efecto?

Yo te diría que si quieres entramos en detalle, pero sí la pregunta es…. hagámoslo simplista. ¿Qué le pasaría a un banco desde el punto de vista criminal? yo te diría coge el Código Penal ves artículo por artículo y te diría que todo, que pasa de todo. Yo me atrevería a decirte que en los 27 o 28 años que he estado a la dirección seguridad del Banco de Sabadell trabajando en diversas posiciones dentro de ella, he tenido la suerte o la desgracia de vivir todo el catálogo del Código Penal completo. Hemos tenido la suerte de por ejemplo no haber sufrido ningún asesinato, pero heridos sí, extorsiones también. Otras entidades financieras han tenido empleados asesinados durante atracos o por la locura de un cliente que entra con una escopeta, … en Cataluña hemos tenido algún caso, todo y que la entidad matriz no fuera catalana. Atracos con muertos ha habido, pero sí que es cierto que cada vez menos. Atracos con heridos hay, clientes que se les ha ido la cabeza y van contra los empleados o directores de oficina, y les hacen culpa de sus problemas económicos hay, robo de todos los tipos hay, fraudes y estafas de todos los tipos hay. Desde el momento que el ciudadano de a pie es víctima de fraudes como el tocomocho la estampita…estás expuesto a que te pase

5.- ¿Cómo está estructurado el departamento de seguridad?

Yo te hablaré de cuando yo estaba que hace un año y poco. Evidentemente ahora me consta que ha cambiado porque cada responsable tiene sus criterios ….

Y te diré de más… que es muy difícil encontrar dos departamentos de seguridad iguales en los bancos porque la historia de las direcciones de seguridad la establece la historia de esa entidad y la historia de las personas que trabajan en seguridad. Esto implica que la Dirección de Seguridad tenga unas funciones y otras. Todas tienen el estándar básico que es vamos a proteger el banco o la entidad que sea y evitar que sufra el máximo de hechos delictivos posibles y los que no podamos evitar que sean lo más poco perjudicial a nivel económico y a nivel reputaciones porque la reputación es un aspecto cada vez más importante porque hoy en día con las redes sociales y su afectación al valor de la acción…. cada vez más el valor reputacional se ve afectado. Entonces lo que tienes que tener es muy bien cubierto los aspectos delictivos y minimizar al máximo su posible comisión y aceptación.

En este sentido la estructura que teníamos creada era … teníamos tres ámbitos muy importantes. Uno era de gestión interna, contratos, calidad, estadística, toda esta parte de asesoramiento y de soporte … Y tenemos otra qué era la parte de seguridad física electrónica, y

otra que eran hechos delictivos como si fuese la típica comisaría que gestionarse los atestados directivos.

El ámbito físico electrónico físico tenía dos componentes físico personas y físico edificios oficinas bancarias patrimonio, ... y físico también podríamos determinar que eran las medidas de seguridad sobre los medios de pago. En muchos casos se separan lo que es la seguridad tecnológica de la del resto de seguridad e históricamente la tecnología tenía muy poca vulneración porque casi no existía. Se ha desarrollado mucho durante los últimos años y está aumentando exponencialmente su incidencia porque vine de cero. El resto de tipologías delictivas están bajando. La seguridad física electrónica tenía un ámbito que se encargaba de la seguridad de la alta dirección otra que se encargaba de la seguridad física de protección física y de las barreras físicas de los edificios y oficinas y la otra la electrónica. Teníamos una persona experta en temas electrónicos y en otra en temas físicos.

La gestión de hechos delictivos como otro ámbito (la comisaría dentro del banco) que era donde se gestionaba cualquier incidencia delictiva que pudiese ocurrir en el banco afectará a quien afectará. Ellos abren su expediente y tratan de determinar cuál ha sido la causa, qué es lo que ha fallado si era un tema que ya tenían previsto y tenía en el procedimiento aplicado para intentar evitar o minimizar el impacto económico o reputacional de este hecho delictivo y si no estaba qué es lo que había fallado intentar de que en un futuro no fallara…

Esta estructura es muy similar a muchos departamentos de seguridad, pero siempre encontrarás otras estructuras en otros bancos a las que se hace de más o de menos gestionan más o menos cosas en función de listón que la empresa determine.

Interpreto que las nuevas amenazas que te marcan la estructura para poder dar respuestas y hablando de amenazas es la tecnología la que te está aportando estas nuevas amenazas. me gustaría destacar estas dos variables Que incorporaremos una es la ciberseguridad y la otra la inteligencia. yo vengo del mundo tecnológico precisamente en el departamento de sistemas entonces me ha sorprendido mucho el banco es un caso, pero no es un caso aislado que en el que la ciberseguridad se lleve desde el departamento de sistemas y no desde el Departamento de Seguridad. a todos los efectos es extrapolable a que una empresa se hace o se haga su auditoría saldrá bien sí o sí. yo principalmente esto lo atribuyo a un desconocimiento en toda la sociedad. sucede una paradoja y es que hacemos servir la tecnología y el nivel de conocimiento que detrás de ella ese mismo.

Yo si me lo permites Abel lo veo un poco diferente que tú, y entroncaremos haciendo un comentario de lo que acabas de decir, sí una empresa se hace su propia auditoría. Nosotros hacemos auditorías de seguridad. Esto no tiene que ver si las quieres complementar con otras externas para durar una visión diferente a la que tú quieres dar o la que tú estás dando. Si somos puristas lo importante es que no sea el mismo que implanta la seguridad Física o electrónica que la persona que las audita, sino una persona diferenciada. Yo creo que estas auditorías son efectivas. Son efectivas y te ayudan a evidenciar los problemas que puedas tener. Yo no le puedo decir al mismo técnico que me instala una electrónica en la oficina que me haga la auditoría, pero sí que se lo podré decir a la misma empresa que tendrá otro departamento que puedo hacer estas cosas.

Yo te diría que muchas empresas que tenemos Departamento de Seguridad hacemos muchas auditorías y cosas de control interno y nos ayuda mucho. Lo complementaremos cómo hacen muchas empresas con el mystery shopping, pero igualmente tenemos un papel importante a jugar.

Cuando tu hablabas de la seguridad tecnológica o ciberseguridad porque tiene muchos nombres yo te he dicho al principio que la historia determina el cómo y porqué está diseñado un departamento de seguridad es decir es la historia quién determina cómo está creado este departamento. Evidentemente cuando nuestra casa se empieza a denotar que hace falta tratar el tema de la seguridad tecnológica o de la informática en aquella época lo que es ahora conocido como si ciberseguridad pensamos nosotros Departamento de Seguridad en qué somos expertos, ¿somos ingenieros electrónicos? ¿Somos ingenieros en telecomunicaciones? sí que hay alguno, pero no son expertos informáticos. Entonces cuando el banco empieza a tener la necesidad determina que se cree el núcleo inicial para regular algunas cosas de seguridad tecnológica dentro de la división de tecnología. Esto provoca que se desarrolle sin prever que podría de ser tan importante. ….

Todos aquellos aspectos tecnológicos, aquellas actividades delictivas de origen tecnológico y otras que están en el límite de ser consideradas tecnológicas incluso acaban yendo hacia el lado tecnológico porque al final pertenecen a ámbitos diferentes dentro de la misma estructura empresarial cada uno empieza o intenta a ganar su propia parcela.

No es por un tema de egoísta sino pensando en que tu formación ayer te ayuda a estar más protegido.

Sí partiremos de cero y hoy en día cerramos todos los bancos y extrapolando lo a otras empresas sí todas arrancaran de cero seguramente lo haríamos de otra manera e incorporaríamos la Ciberseguridad dentro del departamento de seguridad. Es en la asociación que estuve de seguridad integral siempre hemos pensado y hemos apostado por una seguridad integral. Parece que por aquí van los tiros, incluso en las infraestructuras críticas.

Esto también tiene que ver con las personas y con su formación Y en el núcleo que dónde empiezan a haber incidencias, (la tecnología) que estaban separadas del ámbito de dependencia funcional y jerárquica de las divisiones de seguridad y han provocado esta diversa ubicación orgánica que en algunos casos se ha regulado o se ha reconvertido, pero serán muy pocos los casos de bancos y no bancos que el 100% toda la seguridad tecnológica o ciberseguridad depende de la Dirección de Seguridad. Pueden regular algunos aspectos no todos de momento y siempre defenderé como siempre lo he hecho que se ha de hacer una gestión integral y englobando también la seguridad laboral todo lo que tenga que ver con la seguridad por un tema de eficacia y eficiencia. Será mucho más eficiente tener una visión global y transversal de la seguridad que no trabajarlo desde compartimentos estancos por mucho que se esfuercen después en decir que ya existe un comité transversal de seguridad que trate todos estos temas. Esto es mejor que nada, pero la eficiencia no es la misma.

6.- Hablemos de inteligencia, hay mucha teoría sobre lo que es la inteligencia y cada uno tiene su cosa decir. Me gustaría saber qué es para ti la inteligencia y cómo se íntegra en el departamento de seguridad si es que está integrada.

A mí el nombre no me ha gustado nunca. Es como cuando los compañeros te trabajan en el retail hablan de pérdida desconocida que es el hurto que los clientes o empleados causan en el estocaje del supermercado o de la tienda de ropa …

Aquí pasa lo mismo, ¿qué quiere decir, ¿que hasta que no hemos creado un departamento de inteligencia ¿no hemos sido capaces de analizar qué es lo que estaba pasando y a determinar medidas de intervención y de protección para evitar minimizar lo que pasaba?

Esto se ha hecho siempre, esto es la madre del porqué de la existencia del Departamento de Seguridad que no ha de ser reactivo sino preventivo. Y la prevención en seguridad se le llama inteligencia por eso te decía que no me gustaba mucho este término. A partir de aquí nosotros hace años qué hacíamos esta inteligencia sin decirle como tal. El departamento hechos delictivos cuándo analizaba una incidencia veía qué había pasado, cómo lo teníamos regulado si es que estaba regulado, qué se había vulnerado o qué daño se habían producido y cómo lo soluciona …vamos esto junto con la casuística y de las estadísticas y la suma de todo lo que pasaba en todo un año en un territorio en una filial en un continente o en todo el mundo provocaba que tú acabarás determinando dónde hacía falta localizar más o menos medidas en un determinado procedimiento.

Inteligencia siempre hemos hecho y la considero mucho y muy necesaria porque creo que es intrínseco con el nombre del departamento y de una función estricta del Departamento de Seguridad qué es mirar de prevenir que te pasen cosas y las que no puedas prevenir minimizar el impacto al máximo posible. Siempre hemos hecho inteligencia lo que pasa que ahora está de moda tener grandes departamentos con grandes aplicativos... Esto está muy bien, pero yo siempre seguiré defendiendo siempre cambia el nombre de inteligencia no me gusta.

Yo aquí tengo otra teoría con lo que respecta a la inteligencia y es que cada vez más la empresa privada tiene cada vez más recursos para acceder a estas fuentes y para trabajar con estas fuentes. Cuando digo más me estoy refiriendo a que tienen más recursos y más tecnología que la pública para poder explotar esta información y obtener está información y muchas veces muchas veces ya me lo han confirmado mucho antes que les llegue vía seguridad pública es decir voy a policía. Y es esta situación de ventaja la que creo que cambiará la relación entre la parte pública y la parte privada. Veníamos de una subordinación ahora hablamos de una complementariedad de iure y pienso que está ventaja qué aporta la inteligencia a la parte privada la pondrá en una situación privilegiada respecto a la pública y por tanto esta relación cambiará. me gustaría saber cuál es tu opinión al respecto

A mí me gustaría decir que... no me gustaría confundir, … tú puedes llegar a ser muy eficiente porque tiene más herramientas y a lo mejor la administración pública no se preocupará tanto de según qué tipología qué afecta básicamente a las empresas privadas mientras no sea una preocupación o un riesgo qué preocupe al grueso de la sociedad. La ventaja de la empresa privada es que trabajamos sobre la casuística exacta de lo que nos está pasando y podemos

tener herramientas el mercado pone al abasto de todo el mundo con pequeñas adaptaciones yo te diría que el 80% de estas aplicaciones informáticas o estás herramientas de trabajo y de los expertos que pueden contratar nos pueden ayudar pero yo diría que herramientas en el mercado ahí y que la administración se alguna cosa tiene es que tiene grandes recursos y no olvidemos que también tiene grandes profesionales de la seguridad que pueden ser igual de buenos que los de la empresa privada no digo ni mejores ni peores digo igual es. Dales herramientas y evidentemente la empresa privada no tendrá el volumen de negociación que tiene una empresa pública la de comisarías por toda España…. a lo mejor yo pienso qué tal vez discreparía y pienso que nunca, que la empresa privada esté por encima de la pública porque siempre primará el factor que te he dicho al principio. Este factor de es que yo soy la administración y tú estás subordinado a mí.

La realidad es que al final tú puedes ganar en eficiencia porque algunos gestores públicos piensen que no hace falta invertir en este tipo de aplicaciones o en grandes despliegues de profesionales de la Seguridad Pública dedicados al análisis de cierto tipo de tipologías delictivas que no crean una gran alarma social. Los que crean alarma social no te preocupes porque detrás de los cuerpos de policía están los políticos y ya se preocuparán de que cuando un ilícito delictivo cree alarma social por temas de sexo u otros ….

Es lo que pasó con el repunte de accidentes laborales hoy en día con lo normativa se ha conseguido una eficiencia buenísima.

Yo aquí también añadiría en el caso de riesgo laborales y de otros ámbitos que la transposición de directivas europeas contrarresta a veces la pasividad y escaso interés para ciertos ámbitos, ….

Siempre he sido bastante reacio a la excesiva normalización de cómo te has de proteger. Evidentemente, delitos que generen una gran alarma social tiene una cierta lógica que la administración se preocupe para minimizar su impacto y para que la sociedad deje de preocuparse de ella, pero….

En definitiva, soy poco amante de la excesiva regulación, y soy más amante de decir: escuche señor de la administración a quién más le preocupa que mi empresa no le pasa nada soy yo porque me juego el sueldo; usted no. Entonces el dedito que pasa en una entidad financiera o una empresa de retail no creará gran alarma social y por eso soy partidario de crear poca

legislación y dejar a cada uno que decida como gestiona o regula sus bienes. A nadie se le obliga a que tenga una alarma en su casa, ... y la delincuencia domiciliaria no es poca cosa.

Intentar regular como un banco o como en otro sector, intentar entrar en el detalle de cómo te tienes que regular corres un riesgo que …o monitorizas mucho el mapa de riesgos y vas adaptando la normativa cada pocos años en base a estos mapas de riesgos o si no te pasará como nos pasa nosotros que somos el sector más regulado por toda la normativa de seguridad privada que regula la administración. Y te diría que somos los que menos cosas nos pasan estadísticamente hablando. Hay empresas de otros sectores que ellas solas tienen más robos otro tipo de delitos que todas las oficinas bancarias españolas. En cambio, como en su día los deditos asociados oficinas bancarias creo mucha alarma social… el problema es que todo esto ya ha pasado a la historia, pero la regulación si te fijas de atracos es la más extensa.

Seguramente no estoy seguro, pero es posible que digan es que si no llega a ser por esta regulación habría muchos más hechos ilícitos, ...

Sí, pero si te miras los cambios que habido en la normativa y te fijas en lo que hemos hecho las empresas privadas para minimizar los hechos delictivos seguramente te des cuenta que hagamos muchas más cosas que la ley dice que hagamos. Es evidente que la administración diga que gracias a su legislación nosotros hayamos bajado nuestras estadísticas delictivas.

Imagínate que eres el director de recursos humanos del banco y el Presidente o quien sea te dice que tienes que contratar a un director de seguridad. La pregunta es: ¿qué buscarías en este director?

Buscaría experiencia, ilusión, buscaría modernidad desde el punto de vista empresarial es decir dejándonos de antiguas escuelas, de antiguos Tabús…

Es evidente que la experiencia, a no ser que vayas a buscar a gente que esté trabajando. Esto entronca a la inversa de lo que te acabo de decir antes. Que si la persona que ocupa el sitio no venga del mundo de la seguridad sino de la banca...

Otras empresas pueden pensar que si tienen un gran equipo de gente experta en esa materia solo necesitarán un líder que los coordina y no le haga falta alguien que sepa en seguridad. ….

Pero al final como te tienes que acabar enfrentando hablando con la administración con cuerpos policiales la experiencia en este sentido y no hablo de edad sino de bagaje es un gran valor añadido.

Si me permites un paréntesis esto dice mucho de la cultura que hay del concepto de seguridad que tiene una empresa, ¿a quién pones a cargo? Para mí es una aberración poner una persona que no tenga conocimientos porque creo que evidentemente el director tiene que ser un buen gestor, pero tiene que tener el conocimiento. y esto es transversal a todos los ámbitos de dirección en la empresa es una opinión personal.

La ventaja en esto, la ventaja de que, que a lo mejor puedes pensar que se ha puesto en la empresa X una persona que no viene del sector… yo te diría que una de las cosas buenas de esta empresa es que hemos sido capaces de inculcar una gestión y una percepción y vivencia del nivel de seguridad mínimo que requiere tu actividad, con lo cual tú estés donde estés un nivel de seguridad y una preocupación por implantar la seguridad dentro de tus procedimientos y tus productos, está madurez es tan importante que cualquier directivo o cualquier perfil directivo del banco creo que a pesar de no ser un experto en el día a día de la seguridad tiene una cultura de prevención del riesgo o de trato de riesgo de tratar el riesgo y de minimización de riesgo que también es un valor añadido. No tendrá la experiencia del día a día con la gestión delictiva …. en nuestro caso la casa a vigilado mucho Para que dentro de cada nivel en función de los productos son los impactos que pueda tener en la cuenta de resultados con la reputación de la entidad, todos han vivido y se les ha insuflado una prevención del riesgo importantísima.

Hacemos un paréntesis porque esto es cultura de seguridad y sería la última pregunta, pero antes de abordarla y complementando la anterior es comentarte que parece que cada vez más en parte motivado por lo que hablamos antes de ciberseguridad y de inteligencia, el perfil del director de seguridad o el que parece que se perfila como el futuro perfil de director de Seguridad es un perfil mucho más técnico.

¿Qué es Técnico para ti? **Bien pues una persona con la mentalidad ingeniero y conocimientos de seguridad …. me gustaría saber si tú estás de acuerdo en todo esto.**

Yo creo que no necesariamente porque un ingeniero a una persona que evidentemente está acostumbrado a trabajar por proyectos, aunque la seguridad en sí es un proyecto global compuesto de muchos proyectos, si quieres tantos como cada uno de los aspectos que hemos dicho antes lógicos y físicos electrónicos operacionales y dentro de cada uno a lo mejor también algunos subproyectos. Si algunas entidades lo ven desde punto de vista yo te diría que no es un mal enfoque pero como decíamos antes cómo te tienes que ganar esta complicidad sobre todo con la administración, la administración siempre bien y mejor la interrelación o el tú a tú con

un nivel de correlación o colaboración con personas que hayan trabajado en el sector de la seguridad y una persona que por mucha formación que tenga no sé cuántos grados de ingeniería no sé cuántas especialidades y que acaba de salir porque acaba de hacer el curso que a lo mejor es de pocos meses para tener la acreditación director de seguridad, puede ser, serán más reacios a este tipo de figura que no por el contrario con alguien que venga el mundo de la seguridad. Por eso te he dicho antes que le pediría modernidad y modernidad es esta eficiencia y esta forma de trabajar evidentemente si tú quieres relacionada con la ingeniería, pero no necesariamente. Es más, yo soy de formación de derecho y puede ser…. no he hecho del todo un mal trabajo en este mundo de la seguridad por esto yo te digo que más que la formación de base que tenga es que es lo que te deja hacer la empresa que es lo que eres de convencer a la empresa de lo que hace falta hacer y con qué equipo te rodeas para intentar formar el departamento.

Abordamos la última pregunta y tiene relación con lo que has estado hablando reiteradamente, y es la cultura de seguridad cómo función del director de Seguridad en el sentido como tiene que impregnar de esta cultura y cómo se tiene que relacionar no sólo con la persona a la cual reporte sino a toda la estructura de la corporación. Me gustaría que me dijeras cuál ha sido tu experiencia como experto en este ámbito.

Te he insistido bastante en que los directivos de nuestra empresa que vienen de ámbitos que no tiene nada que ver con la seguridad pero han vivido una cultura de seguridad importante y en este sentido yo no quiero decir que sea un mérito mío sino de la propia empresa que me lo puso fácil en el sentido de decir hemos aprovechado la estructura del organigrama de nuestra entidad, qué evidentemente en una entidad como la nuestra con dos mil y pico oficinas y más de 20000 empleados en España y la división de seguridad está ubicada aquí, no tenemos delegaciones de seguridad en cada provincia cómo es el caso de otras entidades financieras. No lo hemos tenido porque nos ha parecido que no hacía falta ni proponerla porque hemos querido aprovechar el modelo básico qué es aprovechar la estructura orgánica, las direcciones corporativas, las direcciones de red territorial para tener dentro de cada uno de estos ámbitos personas a las cuales además de sus funciones estrictas de negocio que determina la organización le daremos funciones de seguridad, de delegación de gestión y de control y de hacer llegar el mensaje a la capa más baja de su territorio, son los directores de cada ámbito

corporativo los encargados de hacer bajar a sus integrantes hasta llegar al perfil más bajo esta cultura de seguridad, y la impregne en sus tareas aunque sean administrativas.

Nosotros escogemos a los directores de cada ámbito y a los directores territoriales y de las oficinas siempre un perfil directivo porque esta persona primero tiene una cierta autoridad hacia todo lo que está debajo... esta autoridad es necesaria.

Por otro lado, tú te beneficias de esta estructura orgánica del organigrama de la empresa para poder llegar hasta abajo pero como no te los hagas tuyos, como no tengas está complicidad, ...

Se trata de hacer partícipes a estos directores. ... al final de no olvidar que la incidencia delictiva tiene un componente económico que afecta tu cuenta de resultados.

Es decir, si tú en tu oficina tienes una normativa de seguridad que intenta no obstaculizarte del todo llegarás aquello de la parálisis por el análisis a ver si después de tantas medidas de seguridad resulta que para poder entrar clientes a tu oficina de vender productos de los cuales el banco y de. también dentro de un mínimo de seguridad porque si ese producto es muy vulnerable los clientes no lo querrán.

Si eres muy vulnerable te estoy afectando la cuenta resultados por tanto está macro visión y macro implicación de todos los estamentos de la cultura provocan que en nuestra casa no necesitemos tener delegados provinciales o gente distribuida por el territorio como tienen otras entidades que es totalmente loable y a lo mejor si te los hubieran dado los hubieras cogido y te estaría hablando de las virtudes de este sistema pero como por lo que sea ni nosotros hemos considerado necesario ni la entidad tampoco lo ofreció buscamos este punto de equilibrio en el cual nos encontramos cómodos y que las estadísticas delictivas determinaban que no fuéramos los peores porque de hecho durante muchos años hemos sido los mejores. Sí estamos en el rango bajo de incidencias delictivas por número y por repercusión económica esto significa que la nuestra posición no ha estado o no ha sido del todo mala y en cambio no hemos tenido esta estructura súper dimensionada.

Nosotros hemos decidido esta fórmula, cogemos a nuestros directivos y contando con su complicidad los sentamos todos juntos y les explicamos que, dentro de sus responsabilidades, y de hecho cuando recursos humanos les marca un mapa sobre cuáles son sus actividades hay un apartado de seguridad. Velar porque se implanten las medidas de seguridad. y esto, ¿cómo me repercute? hombre no vas a tener un plus por esto …

Bien a lo mejor no es un plus directo, pero sí que lo es indirecto no porque no tendrás tantas pérdidas.

11.9 Entrevista Sergi Vivancos

FICHA TÉCNICA	
Descripción	Entrevista a Sergi Vivancos, departamento seguridad Caixabank
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector.
Fecha	16 de -abril del 2018
Lugar	Dependencias CaixaBank
Observaciones	

1.-Sergi, no nos conocemos … la primera pregunta me lleva a saber más de ti. Cuál ha sido tu trayectoria profesional hasta llegar a estar donde estás. ¿Cuál ha sido el recorrido?

Bien yo vengo del cuerpo de Mossos d'Esquadra en el cual entré en el 1986 como Mosso d' Esquadra y aquí en La Caixa entré en el 2008 para llevar la seguridad de los edificios de la Fundación bancaria. Lo que pasa que después me han ha aparecido nuevas tareas como es el tema de la supervisión de los temas de seguridad privada y la interlocución con los cuerpos policiales a raíz de las inspecciones que nos hacen en nuestras oficinas y después la interlocución con el cuerpo.

¿Qué es lo que te hizo dar este cambio pasar de la seguridad pública a la seguridad privada?

Bien al final fue el reto que supone el proyecto de entrar aquí, llevaba 22 años en la seguridad pública y el hecho de venir a una empresa privada evidentemente me atraía mucho ver cómo se trabajaba en la empresa privada de la magnitud de lo que es una empresa como La Caixa y evidentemente la mejora de salario que también evidentemente tiene mucho que ver.

2.- ¿Por qué crees que los ex miembros de los cuerpos de seguridad están ocupando los cargos de Dirección de Seguridad de las empresas y cuál es el valor añadido de estos policías?

Básicamente primero de todo creo que es por la experiencia que una persona que ha trabajado en un cuerpo policial puede dar y puede rendir en una empresa privada, su experiencia es muy importante para poder reconocer a los conflictos las respuestas que pueda haber y después también los contactos y relaciones que pueda haber tenido con estos cuerpos policiales porque delante de una tarea como la que es la de director de Seguridad muchas veces dependiendo de la edad que tengas necesitas el soporte y el apoyo de los cuerpos policiales y si tú ya has trabajado en un cuerpo policial te hace tener estos contactos y al mismo tiempo disponer de las dos vertientes y eres capaz de comprender mejor cuando un policía te dice una cosa y esto te ayuda muchísimo el haber trabajado en un cuerpo policial o.

Diríamos entonces que el valor añadido de un ex policía es en primer lugar el conocimiento adquirido por su experiencia y en segundo lugar también debido a los contactos

Sí y tercero también la visión de la doble vertiente de que tú has ido ya policía que es mi caso. Yo he estado en el lado público y ahora estoy en el privado y me pongo en la piel del policía cuando me dice una cosa e intento entender y así todo es mucho más fácil porque tú ya has estado allá.

Si hacemos un repaso a lo que ha sido el contenido legislativo básico y troncal en materia de seguridad privada dónde tenemos la ley del 92 derogada después por la 2014, hay una clara diferencia entre la relación de las dos seguridades, la privada y la pública desde el punto de vista en el que la ley del 92 situaba la seguridad privada por debajo o subordinada a la seguridad pública. Parece ser que la nueva ley esta relación la intenta equilibrar y hablar de colaboración y corresponsabilidad. ¿Tú crees que hay una diferencia de iure y de facto en esta relación?

Bien yo creo que está bien lo que quería hacer es suavizar un poquito el vocabulario en el sentido de que antes decía que estaba sometida y ahora habla de colaboración, pero evidentemente la seguridad privada está sometida a un control y a una supervisión por parte de la seguridad pública clarísimo. Yo entiendo que lo que ha querido ha sido darle una visión y un concepto diferente, pero en la práctica entiendo que es exactamente lo mismo.

¿Cómo vaticinas esta relación de cara al futuro?

Últimamente tanto la Policía Nacional como los Mossos d'Esquadra están utilizando unas herramientas de comunicación, explicando cosas, los modus operandi, por ejemplo la red de colaboración de Mossos d'Esquadra y Policía Nacional La red azul la Guardia Civil con Copera todo esto son todo esto sí que a diferencia de antes se está haciendo una tarea mucho de

comunicación con los departamentos de seguridad que las empresas de seguridad, detectives privados… Comunica más tipos delictivos modos operandi etcétera pero evidentemente todavía no estamos … dijéramos a la altura de las necesidades que ellos tienen versus las empresas privadas. Nosotros en La Caixa es posible que a lo mejor hay 1000 solicitudes de imágenes al mes por parte de todos los cuerpos policiales. Tenemos dos personas destinadas única y exclusivamente a esta gestión de las imágenes y después a otras consultas relativas a investigación tanto policial como judicial.

Si estuviera en tus manos, ¿qué modificarías de esta relación qué es lo que le falta?

Bien la verdad es que es difícil, seguramente sería incrementar la participación, y la comunicación desde la policía y desde las entidades financieras … ha mejorado, pero tal vez debería ampliarse y regularse porque a veces nos genera un trabajo enorme, y entiendo que es una utopía, porque la policía tiene que investigar y necesita mucho de nuestra ayuda. Lo que pasa que desde mi punto de vista ahora que estoy aquí creo que a veces abusan un poquito demasiado.

A lo mejor es que no tienen otros medios

Yo más bien diría que no los tienen y es mucho más fácil recurrir a nuestros medios. A veces pienso … hombre si aquí tienes otro hilo del cual tirar, pero es mucho más fácil recurrir a nosotros….

Es muy curioso y te comento lo que estoy viendo en el resto de entrevistas de directores que provienen del sector público como tú y de directores vienen de seguridad privada. Este tipo de perfil de director de seguridad es que lo que encuentran a faltar en esta relación es confianza me refiero al sector privado que demandan más confianza por parte de la seguridad pública

El hecho de que el director de La Caixa y yo hemos sido policías, está perdida de confianza queda minimizada bastante porque ellos saben que tú has sido policía. Cuando un policía te pide una cosa entiendes perfectamente lo que hay y también entiendes porque yo he estado al otro lado les que los policías menosprecian la tarea de los directores de seguridad que no han estado a policías porque tal vez les falte esta formación qué es muy importante se trata de la formación policial. Considero que sí que existe, pero en mi caso no he notado esta desconfianza sobre todo por parte de la gente que sabe de dónde provengo. Sí que es cierto que cuando le esta gente no sabe dónde vengo la situación cambia y de hecho hay veces que les tengo que decir

esto no hace falta que me lo expliques porque yo ya lo sé ya he sido policía y noto que esta relación cambia. Cuándo yo hablo con algún policía nacional de la provincia que sea y al final de la conversación le digo que yo he pertenecido a la policía parece que la relación fuera más clara como si estuviéramos hablando entre compañeros salvando las distancias. De alguna manera nosotros tenemos que hacer lo que ellos nos digan ellos son la seguridad pública. Pero muchas veces el hecho de haber estado en la policía me permite rebatirles según qué respuestas o qué requerimientos ordenen y además porque yo he estado en el área de seguridad privada dentro de la seguridad pública y conozco la normativa y la forma de hacer y pensar de la policía.

Eres director de Seguridad de la Caixa se podría decir …

No, yo tengo el título, pero no estoy ejerciendo como director de Seguridad estoy dentro Departamento de Seguridad.

Mi día a día es como el de mucha gente, mirar correos, recibir llamadas telefónicas contestar todos estos correos y requerimientos que me han hecho especialmente en los de la Fundación La Caixa. Piensa que tengo 9 centros que dependen de mí en cuanto a seguridad repartidos en Barcelona, Tarragona Gerona y Lérida Zaragoza Madrid Palma y Sevilla. Yo no estoy en cada uno de los sitios, pero estoy en todos de alguna manera tengo que estar en todos porque ahí hay un servicio de vigilancia y estos vigilantes me reportan novedades problemáticas incidencias sea de lo que sea y evidentemente tengo que dar respuesta.

¿Cuáles son las amenazas recurrentes a la que se tiene que dar respuesta día a día?

Bien hay un sinfín de amenazas desde el punto de vista de seguridad operativa por ejemplo atracos, indigentes qué es muy difícil de resolver este problema, problemas de fraude de cheques de línea abierta, tienes problemas de ocupación de oficinas qué es lo que se lleva ahora por plataforma de refugiados por la hipoteca. Realmente la entidad de Caixabank al tener casi 5000 oficinas repartidas por todo el estado pues tienes una cantidad de incidencias y de vandalismo…. tienes clientes que no están contentos o tienes gente que por lo que sea ve CaixaBank como un enemigo porque es catalana etcétera. El motivo al final es lo mismo es lo de menos, pero problemáticas infinidad al día.

¿Crees que estas amenazas continuarán siendo las mismas?

Bien hay ciclos, Hace años hablamos de 100 atracos al año y hace un par de años 34 o algo así con lo que hemos bajado mucho el número de atracos. Pero por otro lado surgen otras cosas

como es el fraude, usurpación de identidad y estamos intentando, a medida que te salen las problemáticas nuevas, intentamos resolverlas

Para dar abasto a este conjunto de amenazas y seguramente que te has dejado muchas, ¿cómo se estructura el Departamento de Seguridad de La Caixa?

Bien hay diversas áreas que se encargan de resolver estos problemas. Partimos de la base que hay un director de seguridad, con sus directores adjuntos corporativos y después hay un director por cada una de estas áreas. Esta la seguridad operativa para todo esto que decíamos antes de los problemas de los atracos fraudes… la seguridad instrumental que vela porque las oficinas tengan sus medidas de seguridad, me refiero a las que marca la normativa que tiene que tener una oficina, después tenemos el ISOC qué es como si fuera nuestra central receptora de alarmas, pero qué va más allá de una central porque no sólo nos centramos en las alarmas de las oficinas, sino que hay mucha más faena hacer por ejemplo con el tema del fraude con el tema de la continuidad de negocio. Hay muchos temas que de alguna manera el ISOC obtiene la primera información cuando hay una problemática entonces lo que hace la trata y la deriva a las áreas que ya he comentado. Hay un área que lleva el tema de continuad de negocio desde el punto de vista de seguridad hay otra área que lleva el tema dijéramos de análisis de la información qué podemos tener y que repercutan sobre Caixa.

¿Estás hablando de inteligencia?

Más o menos te estoy hablando de prevención. Hay veces que los problemas lo resuelves a medida que te los encuentras y ahí en otros casos en los que intentas hacer esta prevención entonces para esto necesitas un grupo de gente que haga esta tarea preventiva.

También tendríamos gestión de efectivo etcétera.

Me sorprende un poco que no hayas mencionado el tema de ciberseguridad….

Bien porque Ciberseguridad es un tema que no se lleva única y exclusivamente del departamento de seguridad.

Bien este es un tema que tratar en mi trabajo en especial porque yo vengo del mundo de la tecnología en el cual antiguamente la seguridad se llevaba desde el departamento de sistemas. Era el propio departamento de sistemas que se encargaba de la seguridad en los sistemas. Yo tengo una teoría que viene decir que todo y el uso de la tecnología que se hace hoy en día … el nivel de conocimiento en el mercado de lo que hay detrás de esta tecnología

continúa siendo el mismo que hace muchos años todo y la proliferación de esta tecnología. Creo que este desconocimiento generalizado se da también en las unidades de seguridad de la gran mayoría de las corporaciones y por este motivo la seguridad de la red se esté llevando desde el departamento de sistemas. Por un lado, es la típica mosca cojonera que nadie quiere o que el de mejor dicho al Departamento de Seguridad no quiere y por otro lado es una parcela que ya tiene ganada el departamento de sistemas y de la cual no quiere desprenderse. De alguna manera es como sí una auditoría contable me la hago yo mismo hasta qué punto esto tiene valor y relevancia. Me gustaría que me dieras tu opinión al respecto

Bien a ver si que se lleva algo de ciberseguridad porque de alguna manera tenemos un área que lleva un compañero mío qué hace esta tarea dijéramos de trabajar con otras entidades financieras, con otras empresas que también se ven sometidas a ataques cibernéticos y tienen de hecho un grupo que es el de anti phishing. Es working group que se reúnen dos o tres veces al año para darse este tipo de información y ver qué problemas tienen los demás como los han tratado y pasarse esta información. Tener contactos con las empresas de telefonía para saber qué servidores pueden estar implicados, desde dónde. de alguna manera seguridad sí que la trabajamos.

Si tú me estás hablando de una recopilación de información, pero ¿la implementación de las medidas, o ya no tanto la implementación física como puede ser la aplicación de un parche de seguridad sino todo lo que respecta a la política de seguridad está llevando desde el Departamento de Seguridad?

No aquí lo que hacemos es desde el Departamento de Seguridad es obtener información de posibles problemas que han tenido otras entidades. Ver si el problema que nos está afectando podemos obtener alguna información para poder facilitarla a nuestros informáticos.

Bien ahora hablaremos de para mí uno de los pilares fundamentales de la seguridad corporativa y no es otro que la inteligencia como tal. ¿qué es para ti la inteligencia y cuál es su valor añadido?

Bien la inteligencia es súper interesante es súper relevante por esto que te decía nosotros muchas cosas las hemos parado o las hemos minimizado gracias a tener información previa. A veces esta información te la pueden dar los cuerpos policiales porque ellos tienen sus propios servicios de información, pero la gran mayoría lo hacemos gracias a una faena que se hace desde aquí. Nosotros nos hemos avanzado a problemáticas de ocupación de oficinas porque hemos

visto a las redes sociales pues que podríamos tener una ocupación. A raíz de rastrear las redes sociales obtenemos información y podemos o anularla la problemática o minimizarla.

¿Podremos Decir que se trata del tratamiento de la información para obtener una información de calidad para poder utilizarla como ventaja y anticiparnos a una problemática?

Sí, En la Caixa tenemos un departamento propio dentro del seguridad.

Creo que la inteligencia acabará situando la seguridad a la seguridad privada de facto por encima de la seguridad pública y te explicaré el porqué. Se trata de un problema de recursos básicamente. La parte privada tiene acceso a una serie de recursos y de herramientas que la parte pública es imposible ni en número de efectivos ni por presupuesto. Es esta información que ya se está detectando que muchas veces la tiene de primera mano la seguridad privada y es la seguridad privada quién informa a la seguridad pública. No sé qué te parece esta teoría, pero sí que me gustaría saber si alguna vez habéis tenido conocimiento por vuestros propios medios de situaciones delictivas relacionadas con la seguridad antes de que os llega a ser por los cuerpos policiales

Sí sí totalmente. Nosotros a veces, la seguridad pública no solo trabaja para las entidades financieras sino para muchos otros sectores y en situaciones como por ejemplo la situación política que vivimos ahora se deja de hacer muchas cosas porque el abanico de faena es mucho más grande del que tenemos nosotros aquí en La Caixa. Por lo tanto, sí que de retruque nos enteramos de lo que pasa en el mundo de la ciudad de Barcelona y en Madrid, pero todo va encaminado hacia nuestra entidad con lo que la temática se reduce… y tenemos un grupo de personas que trabaja diariamente y por lo tanto te enteras de cosas que a lo mejor la seguridad pública tarda más en darse cuenta. En el momento que detectamos alguna cosa que pueda ser de su interés como además estamos obligada por ley se lo facilitamos. Lo que hacemos nosotros muchas veces es obtener información y ratificarla con los cuerpos policiales. A veces te dicen déjame que me lo mire y te digo algo. Nosotros al final ponemos la información en común con la policía y ellos nos confirman o no esta información.**Me gustaría que te imagines que eres el director de Recursos Humanos de La Caixa y el presidente te encarga contratar un director de seguridad. ¿Qué buscarías un director de seguridad?** Hombre teniendo en cuenta que ya te he dicho antes… tenemos un plus todos aquellos que venimos de un cuerpo de seguridad puede ser que tirará por aquí o por una persona que tuviese muchos conocimientos de seguridad que no sé si una carrera de seguridad a nivel teórico sí que te las puede dar pero no a nivel práctico

por tanto de alguna manera una persona que tenga una carrera de seguridad en unas cosas superaría a lo mejor a una persona del mundo policial pero en cambio la vertiente práctica hay un desnivel bestial a favor de la persona que ha estado en un cuerpo policial por lo tanto si buscase una persona en una entidad como CaixaBank o parecida un director de seguridad importante para mí buscaría una persona con esta experiencia pero no cualquiera sino una persona que de alguna manera destacará porque dentro del mundo policial hay mucha gente. Sabes muchos perfiles y muchas personas que trabajan en el cuerpo policial. A lo mejor una persona en la escala intermedia no tiene porqué ser peor que la escala superior.

Pero básicamente, evidentemente, y la situación que estamos ahora un director de Seguridad con esta experiencia y además conocimientos de Seguridad informática porque todo pasa por el tema informática seguramente sería ideal.

¿Cómo crees que se debe integrar el Departamento de Seguridad con el resto de apartamentos en la empresa?

Bien aquí dependemos de los medios y lo que sí que es importantísimo en una organización es que el departamento de seguridad esté considerado se le escuche y se le dejé trabajar. Sí estamos en organización … y esto pasa a las organizaciones pequeñas donde el director de seguridad es uno más … como si fuera el de Relaciones Institucionales cualquier otro director evidentemente llega un momento que no se le escucha más por lo tanto…. esto pasa sobre todas las empresas pequeñas. En La Caixa al Departamento de Seguridad se escucha, tiene un reconocimiento importante y por lo tanto depende de quién, depende lo pongas en una rama o en la otra lo importante es que el Departamento de Seguridad tenga peso dentro de una organización y se le escuché y se le deje actuar si no es así malamente.

e gustaría sin que llegarás a reproducir la ley cuáles son básicamente las funciones del director de seguridad desde tu punto de vista

Bueno el director de seguridad son las que dice la normativa como por ejemplo vela por las medias de Seguridad de los establecimientos, la comunicación con los cuerpos policiales, … todo esto te lo dice, pero vuelvo a insistir lo mismo hay directores de seguridad de empresas pequeñas que evidentemente no tienen el trabajo que puede llegar a tener un director de una empresa como la nuestra. Un director de una empresa pequeña puede estar muy encima de los establecimientos que dependan de él en cambio un director de seguridad como por ejemplo CaixaBank que tiene 5000 oficinas sus edificios y sus fundaciones evidentemente no podrá llegar

a todos sitios por tanto deberán delegar muchísimo por lo tanto este director de seguridad aparte de cumplir todo lo que tiene que cumplir tiene que saber tener muy buenas relaciones con los cuerpos policiales saber delegar en tu personal y hacer que toda la gente que esté por debajo suyo trabaje.

En cambio, el director de seguridad de una corporación pequeña tendrá menos gente y será mucho más cooperativo y no tan estratégico porque en una organización como la nuestra la estrategia es fundamental.

Bien ligando está respuesta que me acabas de dar con la anterior me gustaría que me hablaras de una de las funciones a mi criterio que debe tener el director de Seguridad y es el del fomento de la cultura de la seguridad en la corporación es decir cómo hacer que esta cultura llegue ya no sólo a sus subordinados del propio departamento sino hasta el empleado de la oficina de Cazorla en Jaén. Para mí es una de las funciones y tal vez también marca el éxito o no de esta figura, es decir, impregnar a toda la organización de esta cultura de seguridad. qué es para ti la cultura de seguridad y como la integrarías dentro de la empresa?

Evidentemente la sensibilización de la seguridad a los trabajadores de una empresa como la nuestra es muy difícil porque tienen otras prioridades evidentemente. Una persona que está al mando de una oficina y todos sus empleados se les marcan unos objetivos totalmente diferentes a los que tenemos nosotros. Ellos tienen que hacer más clientes que estos clientes contraten los máximos productos que ofrece la organización y por lo tanto el tema de la seguridad es un tema es un tema secundario o terciario ¿por qué?

Porque de alguna manera no es su objetivo principal y por lo tanto es muy complicado. ¿Qué hacemos desde CaixaBank y que creo que es lo que sé tiene q hacer en una empresa?

Trabajamos mucho con la formación y cuando tenemos un problema concreto vamos y visitamos a la oficina, pero básicamente intentamos formar a la gente de los errores que se están cometiendo.

Nuestra entidad dispone de una herramienta que es la intranet en la cual ahí hay procedimientos de cómo actuar a nivel de seguridad, pero evidentemente de esto hay gente que se lo lee hay gente que no se lo lee y aquí las vemos de todos los colores. Hay gente que de alguna manera sabe cuáles son las medidas de seguridad, se ha leído todo el catálogo de medidas de oficina y hay gente que no tienen ni idea de lo que es esto por lo tanto es una cuestión muy difícil.

¿Cuándo hay mucha gente que está pendiente del tema de seguridad? Pues cuando ha sufrido un incidente. Una oficina que ha sufrido un atraco está mucho más sensibilizada que no una oficina que no ha sufrido nunca un atraco.

Ya te digo es que cuesta mucho que la seguridad sea una cosa muy importante dentro de su día a día de trabajo. Es difícil, pero nosotros lo hacemos a través de una intranet y a través de formación desplazándonos a las oficinas porque a la gente se les hace clase de formación explicando cuáles son los problemas y se los intentamos resolver in situ.

11.10 Entrevista Xavier Sánchez

FICHA TÉCNICA	
Descripción	Entrevista a Francesc Xavier Sánchez, director de seguridad adjunto Universidad Autónoma de Barcelona
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector.
Fecha	16 de abril del 2018
Lugar	Dependencias UAB
Observaciones	

1.-Francesc, no nos conocemos … la primera pregunta me lleva a saber más de ti. Cuál ha sido tu trayectoria profesional hasta llegar a estar donde estás. ¿Cuál ha sido el recorrido?

Yo empecé en el año 85 como auxiliar de detective privado. Antes para ser detective privado te tenía que recomendar un policía e ir a Madrid a hacer un examen para conseguir el título. Mientras no tenía esto un profesor de Criminología me dijo que si quería trabajar con él. Estuve con él y después ya entré en un despacho y estuve 15 años como detective privado primero solo y después integrado en un bufete de abogados. Yo tenía mis clientes propios, pero todos los casos en los cuales ellos necesitaban detectives me los pasaba a mí así estuve durante 15 años. De aquí me pasé a seguridad privada por un tema más personal. Yo no tenía horarios

viajaba y no sabía cuándo volvía tuve a mi hija Paula, también tuve un accidente muy grave en moto haciendo un seguimiento.

Lo único que veía que me atraía porque lo mío era vocacional era la seguridad. Comencé desde cero. Me saqué el título de seguridad en la universidad. El primer trabajo que encontré fue en el Hotel Arts, yo no tenía currículum, yo era oficial de vigilancia. Aquí hacía de todo, tenía mucho trabajo y muy variado. Después pasé al hotel Juan Carlos primero.

En el Hotel Arts tenía una coordinadora de seguridad que no tenía el título de directora de seguridad, pero cuando se puso la primera piedra del hotel la vigilante de la obra era ella.

Seguridad dependía del jefe de ingeniería de mantenimiento que era muy típico anteriormente que la seguridad dependiese de mantenimiento.

Pero quien controlaba realmente la seguridad era un ex Seal que había sido jefe de seguridad de la Casa Blanca. Se dedicaba a ir en toda la cadena Ritz Charlton de hotel en hotel comprobando que se compilan los parámetros de seguridad que él había instaurado.

En el Hotel Juan Carlos primero el director de seguridad era un ex policía nacional. Allí estuve de ayudante del director de seguridad. Estuve 5 años.

Después ya se abre una plaza en la Universidad Autónoma, una plaza bajo concurso en la que pedían tener la TIP de director de Seguridad de detective privado. . nos presentamos unos 38 y salí yo elegido.

2.- No es ningún secreto que los puestos de director de Seguridad Corporativa están ocupados por los ex miembros de los Cuerpos y Fuerzas de Seguridad del Estado. Me gustaría saber tu opinión al respecto y también que me dijeras porque se da esta situación

Bien, creo que básicamente hay dos motivos uno es la agenda de contactos y otro por un tema de estudios. Antes no había estudios reglados, sino que simplemente pasaban los ex policías. A partir del momento en que la Tip era obligatoria, los policías empezaron a sacarse la titulación. Esto te demuestra que, …que tardaremos muchos años a que la gente que tenga que decidir qué director de seguridad quiere llegará un momento que busque una persona preparada con vocación.

Entonces podríamos decir que el Valor Añadido sea la experiencia de esta persona en tareas de seguridad y un tema de contactos.

Sí.

Hay una circunstancia que también se da y es que la respuesta que dan los ex policías es una y los que vienen del mundo de la seguridad privada dan otro tipo de respuesta. Normalmente los policías no hablan únicamente de la agenda porque dicen que tiene una caducidad…. Y el resto de personas que han venido del mundo privado como por ejemplo tu caso que dicen que al final los contactos los trabajas tú y normalmente si eres una persona con habilidades comunicativas no has de tener ningún problema para tener una serie de contactos.

Sí, pero si tú coges a una persona que haya estado 15 años en el CNI no puedes competir contra esto. Esto no tendría que ser así, pero … pero es así. En mi caso como fue por concurso esto desaparece. Seguramente si no hubiera sido un tema a concurso yo no estaría dónde estoy.

Cambiamos de pregunta, y hablando de la relación entre Seguridad Pública y seguridad privada, la ley del 92 en la cual la seguridad privada la subordina a la seguridad pública, esta relación de iure se modifica en la 2014 que habla más de complementariedad y colaboración

En el Fondo continúa todo igual porque a nivel de administración y de inspección dependemos de ellos. En mi caso la relación con la parte pública es muy buena, pero porque es diaria básicamente y a los dos nos interesa estar bien.

Aquí en la universidad hay muchos usuarios, mucha gente, muchas procedencias y con el tema del terrorismo dado que tenemos gente de todas las procedencias … comunicación e intercambio de información mucho más. En ese sentido la relación es muy fluida.

¿Dirías que hay confianza??

Mucha, aunque siempre hay algunas veces o alguna persona más reservada que otra, pero por lo general mucha confianza.

¿Cómo crees que evolucionar a esta relación…?

En principio creo que continuará igual…….

-INTERRUPCIÓN TELÉFONO:

Eres director de seguridad adjunto de la Universidad Autónoma de Barcelona, me gustaría que me dijeras cuál es tu día a día cuáles son tus tareas diarias

El día a día normal … entro, aunque no tengo horario fijo, pero entro sobre las 9 de la mañana y lo primero que hago es pasar por sala de control hacer un pequeño briefing para pasar las novedades desde que me he marchado el día anterior hasta que yo he vuelto…. a no ser que hay algo muy importante porque yo estoy 24 horas disponible y entonces ya tendría que venir.

Hacemos el briefing, me comunican las incidencias (el equipo humano que tenemos ese día) y después voy al despacho y si no tengo reuniones reviso todos los informes del día anterior que no he podido revisar antes de irme o antes de finalizar mi jornada laboral. Reuniones de todo tipo, personal de mantenimiento logística autobuses, ferrocarriles, …Hay muchos días en los que tenemos actos preparados como manifestaciones Congresos, VIPS que vienen aquí y después, … tenemos una rutina de control de hurtos de la que se encargan los vigilantes dado que últimamente tenemos lleva esas bandas de peruanos por la zona. Vestimos a estos vigilantes de paisano para que pasen desapercibidos.

También preparo diferentes informes, etc, …

¿Entonces en cuanto amenazas qué tipo de ventas recurrentes tienes que hacer frente día a día?

Al margen del hurto que te acabo de comentar:

Tenemos riesgos internos como incendios, porque tenemos mucho laboratorio tenemos mucho producto inflamable, también tenemos uranio, tenemos lugares que están muy protegidos para que no entre nada y lugares que están muy protegidos para que no salga nada comedias de seguridad muy específicas. Piensa que nosotros tenemos, ... en el último temporal de vientos nos cayeron 2800 árboles, tenemos mucha vegetación y caída de árboles y es importante como riesgo para nosotros.

Riesgos externos hemos tenido que confinar por nevadas hemos tenido que evacuar por vientos. Movimiento sísmico no hemos tenido ninguno, en temas de mercaderías peligrosas no hemos tenido tampoco ningún incidente todo y que tenemos la autopista y ferrocarriles al lado.

Brotes infecciosos, nosotros tenemos granjas de animales de todo tipo de animales también es un riesgo que tenemos que considerar. También tenemos otros riesgos y es que estamos al lado de un aeropuerto, …

¿Crees que este tipo de amenazas girarán hace un tipo de amenazas en concreto?

Bien las amenazas físicas como las caídas de árboles que te he comentado no esto no cambiará. Por el tema del patrimonio básicamente bueno, el hurto y algún robo con fuerza en los domicilios de los estudiantes bien yo creo que todo esto se mantendrá igual. Ahora quizás lo que marque un poco la agenda es la situación política que estamos viviendo en Cataluña y están creciendo los actos vandálicos Reivindicativos.

Nuestra estructura pasa por un director de Seguridad los dos directores de seguridad adjuntos hay otra figura también que tiende a desaparecer qué son los jefes de grupo.

Estos jefes de grupo están por las noches en turnos en los que no están los directores de seguridad. En principio están por si se produce alguna incidencia, avisar a guardia, pero al no haber ningún personal del Departamento de Seguridad se les llama jefes de grupo. Si hay algo importante nos despiertan a mí a la María o a Manel.

después están los vigilantes no los vigilantes de seguridad sino vigilantes que tenemos de la propia universidad autónoma pero poco a poco se está externalizando.

Son una especie de auxiliares de seguridad. Al final personal propio de la Autónoma estamos hablando de unas 30 personas para cubrir todos los turnos.

No me has hablado de ciberseguridad…

Bien a la estructura de seguridad tienes que sumar nuestra empresa privada nuestra empresa privada de seguridad….

Te comentaba que resulta muy curioso que no se lleve la ciberseguridad desde el departamento de Seguridad. Yo tengo una teoría que apunta hacia dos frentes: uno de ellos ya lo hemos comentado antes y es que el Director de Sistemas no se quiere deshacer de su parcela y por otro lugar es un tema endémico de la sociedad y es que a pesar de que cada día hagamos servir más tecnología el nivel de conocimiento de lo que hay detrás en materia de seguridad se mantiene igual.

Bien yo como director de seguridad no tengo esta formación. Estoy totalmente de acuerdo con lo que dices. La primera problemática es, y te hablo de dónde estoy ahora porque por ejemplo cuando estaba en el hotel por hacerlo más pequeño éramos 200 trabajadores y no 5000 tenía su propio departamento de informática y les costaba que nos dieran acceso al listado de clientes sin pasar por recepción era una odisea.

A nivel más global todo el mundo defiende su parcela y me parece bien, pero lo que no puedes hacer es poner un muro egoísta porque si tú lo que quieres es el bien de tu corporación ábrete e intenta colaborar.

En nuestro caso no estamos preparados para asumir ciertas tareas, pero sí que tenemos un personal que le llaman el tic es un cargo de confianza de la rectora que esta marca la tendencia a seguir en cuanto a los servicios informáticos.

Si es que si esto lo extrapolar al mundo contable sería parecido a que una entidad financiera si hiciese su propia auditoría… entonces saldría perfecta. Lo que se tiene que pretender por un bien de la seguridad es que la ciberseguridad esté dirigida por el Departamento de Seguridad y después la implementación de las medidas que se determinen las implemente el departamento de sistemas. Digamos que el departamento de seguridad sería el organismo consultor del departamento de sistemas en materia exclusivamente de seguridad.

Actualmente con los estudios se os prepara en estos temas porque yo no lo tenía ni como asignatura….

Sí nosotros la tenemos como asignatura ….. y además todo apunta a que cada vez el perfil de director de seguridad será más un perfil de ingeniero sin abandonar evidentemente la parte de seguridad, pero sí un perfil más técnico.

Si en un departamento de seguridad de una entidad importante tendrá que configurar muchas áreas por ejemplo el que se encargue más de la parte técnica, aparte de ciberseguridad otro de la parte de sistemas de detección intrusión etcétera.

Sinceramente yo creo que debe ser así y si no fuera así la vida del director de seguridad será corta, es decir, el director de seguridad tendrá que asumir las funciones de seguridad en la parte tecnológica.

Aquí entramos en temas culturales y de intereses, pero esto por el bien de la seguridad debería cambiar.

Hemos hablado de ciberseguridad y para mí otra de las patas importantes de cara a cerrar el círculo de lo que podría ser la seguridad integral es la inteligencia, es decir entendida como el trato de la información, para convertirla en información útil y convertirla en una ventaja respecto al enemigo, es lo que hemos estado hablando antes… redes sociales etcétera la obtención de esta información por vías abiertas sobre todo el tema de OSIINT. Claro en una sociedad que se llama la sociedad de la información y por otro lado decimos que quién tiene la información tiene el poder interpreto que la inteligencia será una de las ramas que debe aguantar la seguridad corporativa juntamente con la ciberseguridad y que con lo que realmente conocemos como si hubiera física. Me gustaría saber tu opinión y si en el caso de la Universidad Autónoma tienes cubierta la parte inteligencia.

Yo recuerdo que antes se buscaban carteles y pancartas en las manifestaciones de los estudiantes y era lo que buscaban los Mossos d'Esquadra y a ver quién colgaba esos carteles en

las manifestaciones, ... lo que antes se hacía con cartelería que también se hace porque tenemos gente desplegada por el campus que nos informa de cualquier incidente desde pintadas carteles etcétera. Ahora también miramos las redes algún nivel básico además ellos ya lo saben, … ellos saben que estamos detrás… y no utilizan mucho el Twitter, pero a pesar de todo sí que tiramos de esta tecnología porque nos ayuda…. Bien hoy en día a través de las redes sociales puedes conseguir hacerte una idea del perfil de una persona. Sí que estoy de acuerdo que es básico, es lo que te digo que yo vengo de la investigación y la seguridad necesita que haya una investigación detrás de cualquier aspecto para no tener que ir siempre a remolque y disponer de una información previa que para mí es básica. Pero si me preguntas en nuestro caso concreto lo que hacemos a nivel de tecnología es muy muy básico.

Bien yo creo que la inteligencia como tal cambiará la relación entre la seguridad pública y la privada. Hoy en día las grandes corporaciones y el sector privado tienen herramientas que pueden explotar cantidades ingentes de información, tiene muchos más recursos para poder realizar esta inteligencia mucho más recurso que la parte pública y al final con la inteligencia obtenemos información y la información es el poder y desde la parte privada se obtiene más inteligencia. Al final acabará situándose en una situación de privilegio respecto a la seguridad pública.

Sí.

Imagínate que eres el director de recursos humanos, aunque aquí en tu caso se tendría que publicitar a nivel de oposición el cargo director de seguridad, pero tú imagínate que está en tus manos escoger a este director de seguridad que buscarías tú un director de seguridad

Muy buena pregunta. Experiencia, motivación, preparación técnica y legal, habilidades para relacionarse y con contactos.

En lo que respecta a preparación es importante todo aquello relacionado con el tema tecnológico

y tú qué piensas?

A lo mejor en una corporación tan grande más que formación lo que tiene que tener es tener una buena visión para poder tejer una buena estrategia en seguridad, pero sí rodearse de grandes expertos en las áreas determinadas.

Claro que el exigido el que una persona tenga tanto nivel de conocimiento en todas las áreas es complicado por eso es importante que sepa gestionar y que se rodee de grandes expertos. Pero sí, el perfil parece ser que cada vez será más técnico.

¿Cómo crees que se tiene que integrar un departamento de seguridad con el resto de departamentos de una corporación? Lo mejor la UAB es una corporación un tanto especial porque es administración, pero lo puedes extrapolar a cualquier otro ámbito

Mi ideal sería que fuese una estructura muy relacionada con todo el resto departamentos. Lo que tengo muy claro es que hasta ahora un poquito más el Departamento de Seguridad …. si miras el organigrama siempre cuelga de otros departamentos por ejemplo mantenimiento esto es una locura. Para mí tiene que estar como mínimo al mismo nivel y a lo mejor por encima de muchos otros niveles. Yo no me considero mejor que nadie… al final todo puede ser atacado y no es estar por encima tuyo por un tema de sueldo ni nada de esto es por un tema de tener toda la información. Tú al final decidieras qué pones o no porque a lo mejor me tienes que consultar a mí porque te puedo decir que en la planta 30 en un edificio de 60 plantas no puedes instalar según qué cosa …

Esto que me estás explicando tiene mucho que ver con la última pregunta … me gustaría que me dijeras no lo que dice la ley porque la puede consultar todo el mundo cuál es el ABC de las funciones del director de seguridad… ¿qué tiene que hacer bajo tu opinión un director de seguridad?

Parlen del security dejamos el safety. Lo que tiene que hacer es proteger la empresa y cuando digo la empresa es todo personas patrimonio y todo. Básicamente con esto ya te lo digo todo cuando hablo de protección es protección integral: información, económica, agresiones fugas de información todo.

Cuando antes decías que no es estar por encima yo sé a qué te refieres… al final y como una de las funciones básicas del director de seguridad como colofón final … es el tema de la cultura de la seguridad, es impregnar de cultura de seguridad a toda su corporación es decir que cuando alguien haga algo tenga un angelito que le advierta de qué tiene que pensar en seguridad

Esto es súper básico a lo mejor no tanto a nivel que tú lo dices, pero te pongo un ejemplo de aquí a 3 meses se acaba la construcción de un edificio aquí al lado. A ver cuando ya esté todo hecho me dirán que ya puedo poner las cámaras los detectores etcétera. A lo mejor si lo tengo que poner como debo poner lo tengo que tirar esto y lo otro y esto no lo puedo tirar porque me has hecho esto. Qué cuesta que esto ya estuviese previsto de antes, que seguridad hubiera participado en el proyecto anteriormente. Hubiéramos ahorrado recursos….. esto no pasa nunca.

Nosotros estamos intentando instaurar esta cultura lo que pasa es que cuesta muchísimo. Al final la gente se mueve por inercias… De todas maneras, tengo que decirte que es avanzado mucho los años que llevo, pero de todas maneras cuesta mucho.

11.11 Entrevista Bernat Baró

FICHA TÉCNICA	
Descripción	Entrevista a Bernat Baró, Director de seguridad del puerto de Barcelona.
Técnica instrumental	Entrevista semiestructurada
Objetivo	Investigar sobre el perfil de un director de seguridad; amenazas recurrentes; estructura de departamento; análisis del sector
Fecha	28 de Mayo del 2018
Lugar	Puerto de Barcelona (Dept. Seguretat)
Observaciones	

1.- Sr. Bernat, no nos conocemos … la primera pregunta me lleva a saber más de ti. ¿Cuál ha sido su trayectoria profesional hasta llegar a estar donde estás...?

De entrada, yo nunca me había planteado desde que entré en Mossos d'Escuadra en el año 83 hacer una función diferente a la que es la policía el estrictamente. Dentro del ámbito policial es verdad que tú qué muchos palos. Pero me gustaría empezar por la última parte, vine hacia aquí un poco por casualidad. Me lo propusieron y es verdad que no tenía mucha más salida policial porque había llegado a comisario que es lo máximo. Me pude ir con una excedencia que me permitía irme de mossos sin perder ningún derecho. Lo que quiero decirte es que no tenía una

vocación diferente a la policía, pero lo que sí que es verdad es que cuando hablamos de gestión o management al final da igual dirigir personas de un ámbito que de otro y por lo tanto lo que hago aquí no es tan diferente de lo que hacía en Mossos. Mi bagaje profesional en unos ámbitos dijéramos que iba no sobrado pero suficiente, pero en otros ámbitos he tenido que aprender enormemente. Empecé en un grupo que se llamaba escamo 16 qué hacía un poquito de todo, investigación, servicios especiales, avanzadas del presidente, después fui a la Brigada de menores y aprendí a hacer de policía judicial. Más tarde empezamos a hacer las primeras entradas a domicilio, las primeras intervenciones telefónicas, las primeras investigaciones. Aquello no sirvió de embrión. Después me hice cargo de la CPOME, después del área de menores, después me hice cargo de los grupos especiales de intervención que son los GEI, subsuelo, canino Tedax,

Después inventaron un área que se llamaba inteligencia que nombre y hace un poco de risa, pero fue a raíz de mi regreso de Estados Unidos después de una formación del FBI y en el año 94. A partir de aquí me di cuenta que inteligencia es un tratamiento de la información, y me di cuenta que lo primero que tenemos que hacer es tener la información en archivos. Organizamos la información del cuerpo de Mossos d'Esquadra en 5 entidades básicas, personas, vehículos etcétera y configuramos el CIPAC de dónde nace el SISD. Poco a poco traspasamos la información del área de menores al CIPAC. Cuándo tenemos la herramienta desarrollada gracias a los informáticos porque nosotros decíamos cómo se tenía que hacer se vuelca todo el sistema de atestados de mossos. Nos damos cuenta que el sistema de atestados es muy lento volcarlo y creamos lo que se llama las marcas, es decir, a través de los atestados ponemos las entidades entidades básicas enmarcar al fin y efecto de no tener que estar introduciendo cada vez esta información de manera manual. La verdad es que fue un éxito y nos lo copiaron en toda España.

A partir de ahí empecé a dedicar a hacer investigación de casos muy especiales, trabajando para jueces de Barcelona cómo fue el señor Aguirre con el que hice mucha amistad. Él nos dio la primera comisión rogatoria para trabajar en Bélgica. Además, él consiguió que pudiéramos entregar las diligencias y detenidos a los juzgados de Barcelona.

Después a partir de aquí me fui a la escuela de policía de Cataluña hice el material didáctico del curso básico de los módulos 3,5 y 7. Lo desarrollamos 3 personas de las cuales una de esta una de esas personas era yo, el único mosso del grupo.

Después me fui a formación del cuerpo y después me volví a ir a Fiscalía de menores, justo antes del despliegue. Después me fui a la Región Metropolitana Norte de subjefe y después bajé a Badalona y mis últimos 5 años fui el jefe del área básica policial de Badalona ni cuándo sale comisario a los 10 días me propusieron hacerme cargo de la Dirección de Seguridad del puerto. Yo dije que me lo pensaría, se lo dije al de l'hort y me dijo que no podía marchar porque acaba de ser escogido comisario y después el conseller me dijo que estaría muy bien en el puerto y en definitiva aquí estoy.

2.- **No es ningún misterio ni secreto que los puestos de DS los están ocupando en un gran porcentaje ex-miembros de cuerpos de fuerzas y cuerpos de seguridad del Estado. ¿A qué crees que se debe, ¿cuál es su valor añadido?**

Entonces podríamos decir que esta situación ha sido originada por la propia Ley de Seguridad Privada qué es un nivel de exigencia para o con respecto al perfil del director de seguridad es un poquito naif y por esto las empresas aprovechan el conocimiento de los ex miembros de los cuerpos policiales para ocupar este lugar…….

De entrada, yo nunca me había planteado desde que entré en mosos de escuadra en el año 83 hacer una función diferente a la que es la policía el estrictamente. Dentro del ámbito policial es verdad que tú qué muchos palos. Pero me gustaría empezar por la última parte, vine hacia aquí un poco por casualidad. Me lo propusieron y es verdad que no tenía mucha más salida policial porque había llegado a comisario que es lo máximo. Me pude ir con una excedencia que me permitía irme de mossos sin perder ningún derecho. Lo que quiero decirte es que no tenía una vocación diferente a la policía, pero lo que sí que es verdad es que cuando hablamos de gestión o management al final da igual dirigir personas de un ámbito que de otro y por lo tanto lo que hago aquí no es tan diferente de lo que hacía en Mossos. Mi bagaje profesional en unos ámbitos dijéramos que iba no sobrado pero suficiente, pero en otros ámbitos he tenido que aprender enormemente. Empecé en un grupo que se llamaba escamo 16 qué hacía un poquito de todo, investigación, servicios especiales, avanzadas del presidente, después fui a la Brigada de menores y aprendí a hacer de policía judicial. Más tarde empezamos a hacer las primeras entradas a domicilio, las primeras intervenciones telefónicas, las primeras investigaciones. Aquello no sirvió de embrión. Después me hice cargo de la CPOME, después del área de menores, después me hice cargo de los grupos especiales de intervención que son los GEI, subsuelo, canino Tedax,

Después inventaron un área que se llamaba inteligencia que nombre y hace un poco de risa, pero fue a raíz de mi regreso de Estados Unidos después de una formación del FBI y en el año 94. A partir de aquí me di cuenta que inteligencia es un tratamiento de la información, y me di cuenta que lo primero que tenemos que hacer es tener la información en archivos. Organizamos la información del cuerpo de Mossos d'Esquadra en 5 entidades básicas, personas, vehículos etcétera y configuramos el CIPAC de dónde nace el SISD. Poco a poco traspasamos la información del área de menores al CIPAC. Cuándo tenemos la herramienta desarrollada gracias a los informáticos porque nosotros decíamos cómo se tenía que hacer se vuelca todo el sistema de atestados de mossos. Nos damos cuenta que el sistema de atestados es muy lento volcarlo y creamos lo que se llama las marcas, es decir, a través de los atestados ponemos las entidades básicas enmarcar al fin y efecto de no tener que estar introduciendo cada vez esta información de manera manual. La verdad es que fue un éxito y nos lo copiaron en toda España.

A partir de ahí empecé a dedicar a hacer investigación de casos muy especiales, trabajando para jueces de Barcelona cómo fue el señor Aguirre con el que hice mucha amistad. Él nos dio la primera comisión rogatoria para trabajar en Bélgica. Además, él consiguió que pudiéramos entregar las diligencias y detenidos a los juzgados de Barcelona.

Después a partir de aquí me fui a la escuela de policía de Cataluña hice el material didáctico del curso básico de los módulos 3,5 y 7. Lo desarrollamos 3 personas de las cuales una de esta una de esas personas era yo, el único mosso del grupo.

Después me fui a formación del cuerpo y después me volví a ir a Fiscalía de menores, justo antes del despliegue. Después me fui a la Región Metropolitana Norte de subjefe y después bajé a Badalona y mis últimos 5 años fui el jefe del área básica policial de Badalona ni cuándo sale comisario a los 10 días me propusieron hacerme cargo de la Dirección de Seguridad del puerto. Yo dije que me lo pensaría, se lo dije al de l'hort y me dijo que no podía marchar porque acaba de ser escogido comisario y después el conseller me dijo que estaría muy bien en el puerto y en definitiva aquí estoy.

3.- Haciendo un repaso al compendio legislativo, y básicamente a la ley del 92, y posteriormente la ley del 2014, ¿cómo valoras las relaciones entre la Seguridad Pública y Privada?? Cómo. ¿Vaticinas esta relación?

Sin ninguna duda primero la interrelación y coordinación entre cuerpos no es fácil porque estamos hablando de 5 cuerpos policiales, Guardia Civil, Policía nacional, Mossos, Guardia

Urbana y Policía Portuaria y si se diera el caso hasta podríamos hablar de Policía Local del Prat. Su coordinación me cuesta alguna que otra comida. La coordinación inter cuerpos será de dos maneras por un tema de territorio o especialidad y aquí será de ambas formas.

Dicho esto, la relación con la seguridad privada y cómo se va a coordinar no os iba a más o menos. Es evidente que va a más, cuando yo llegué aquí el control de acceso a los barcos a los cruceros se hacía a través de la Guardia Civil. La Guardia Civil se dio cuenta de que esto le ocupaba muchos recursos y a petición de ellos y porque nosotros queríamos más agilidad en las operaciones de entrada de los barcos lo que hicimos es suplir la Guardia Civil con seguridad privada por lo tanto el control, igual que en los aeropuertos, de los arcos y de los scanner pasa a través del control de la seguridad privada. Lo mismo nos pasó al cabo del tiempo que el Cuerpo Nacional de Policía y Guardia Civil llevaban perros de detección de explosivos, pero no lo hacían de acuerdo a un modelo universal. Tuvimos una inspección a nivel europeo y nos dijeron que estaba muy bien, pero nos tuvimos que hacer un sistema que nada más lo hace ACESA y el puerto de Barcelona y lo hicimos con los perros de la Guardia Civil. Por lo tanto, bajo la supervisión de los cuerpos policiales y sometidos a la subordinación cada vez hacen más funciones sin perjuicio de que las funciones de acceso de control al puerto que lo hace la Policía Portuaria, es posible que dado que no podemos crecer en efectivos también acabemos externalizando estas funciones. Por lo tanto, cada vez hay más funciones que son delegadas y que se traspasan a la seguridad privada.

La subordinación hola qué hacías mención hace un momento no puede ser de otra manera, lo único es que la palabra no me gusta. Se deben buscar eufemismos para hacer referencia a esta relación. No hay ninguna duda que la seguridad privada forma parte del sistema de seguridad. No hablamos de subordinación son unas tareas que en todo caso que está claro que la seguridad pública no se puede poner subordinada a la privada en ninguno de los casos porque por eso es pública y por lo tanto en todo caso si tuviésemos que hablar de subordinación ya está bien cómo está pero el concepto como tal para mí no es subordinación es colaboración es en todo caso coordinación pero no puede ser una subordinación entendida en el sentido despectivo por lo tanto el sistema de seguridad pública privada todo junto forma parte del sistema de seguridad. De acuerdo que la ley de Cataluña habla de sistema de seguridad pública, pero yo creo que la seguridad privada está muchas veces haciendo funciones en el ámbito público por lo tanto también forma parte del sistema seguridad pública

4.- Eres el DS del puerto de Barcelona. ¿Cuál es tu día a día?

Yo soy director de Seguridad Corporativa. Cuando llegué era director de seguridad operativa y solo llevaba lo que se llama la security y actualmente llevo Security y safety. Safety sabes que es esos hechos que se producen de forma accidental. Por lo tanto, la seguridad industrial, en la emergencia, emergencias médicas de cualquier ámbito. Mi día a día es gestionar los recursos que tiene el puerto en estas tres patas básicamente que son: seguridad industrial, seguridad operativa del ámbito policial, y protección portuaria. Día día me pasó como todo el mundo hoy en día gestionando una media de 90 correos diarios. Esto es una hipoteca horrorosa pero también me permite bajar a la arena, tengo una estructura muy buena, tengo dentro de la policía hay un intendente, una estructura de inspector, subinspectores, por lo tanto, descansa sobre una estructura. Dentro de seguridad industrial controlando los planes de autoprotección, autorizaciones de diferentes eventos, las actualizaciones de seguridad o de safety y los planes de autoprotección de todas las instalaciones, … La supervisión y que todos los servicios tengan los recursos suficientes para llevarlos a término.

Vamos ahora de vulnerabilidad y amenazas. Para saber las vulnerabilidades tenemos que evaluar nuestros riesgos. Es verdad que las vulnerabilidades más graves actualmente son del ámbito que te he comentado de los ciberataques porque se demuestra que es donde nos atacan. De hecho, no es que ataquen al puerto, ellos atacan. ¿Cómo funciona la ciberseguridad? Bien pues ellos atacan y cuando encuentran una puerta abierta normalmente quien la encuentra abierta no es quien quiere acceder al puerto, sino que lo que hace es vender la información que el puerto tiene una puerta abierta.

Después si te tengo que admitir una debilidad o amenaza por lo que respecta al puerto hay ámbitos que están bien cubiertos… nosotros la seguridad la hacemos con círculos concéntricos. Si tú vas al cuore vas pasando por círculos de seguridad que cada vez son más críticos. Por eso he quedado contigo aquí fuera, ... Si fueras aún otro sitio más restrictivo como por ejemplo el muelle de energía hubieras pasado otro sector de seguridad mucho más receptivo todavía y si llegas a la estación X a veces llegado a otro círculo de seguridad.

Información NO QUIERE QUE SEA PÚBLICA POR SEGURIDAD XXXXXXXXXXXXXXXXX

5.- **Estamos en la sociedad que hacemos un uso muy exhaustivo de la tecnología cada vez más pero no hay una cultura de seguridad de lo que hay detrás de todo esto. Esto pasa en todos los niveles no sólo a nivel de usuario sino también de gerencia y hasta nivel de los juzgados**

que no quieren saber nada de tecnología. Entonces yo relaciono esto y se produce una cosa muy curiosa en temas de ciberseguridad y es que la ciberseguridad muchas veces o en la mayoría de las veces no se lleva desde el departamento de seguridad sino desde departamento los sistemas de información y esto a mi modo de entender es como si yo mismo me hago una auditoría de mi empresa, saldrá bien porque me interesa que salga bien. Yo esto lo relaciono con el desconocimiento que hay en los departamentos de seguridad de la propia ciberseguridad entonces me gustaría preguntarle desde dónde se gestiona la ciberseguridad en la Diputación y como cree usted que tendría que ser este modelo

Es verdad ...

No es bien bien por esto. Yo te diría que soy perfectamente capaz de saber las vulnerabilidades del sistema de seguridad informática. Yo las conozco lo que pasa es que no me he formado como informático, por lo tanto, en el fondo la filosofía es lo mismo que te he comentado antes. Ahora bien, el conocimiento de las vulnerabilidades sí que un director de Seguridad las tiene que conocer. Yo tengo que conocer que en este momento te pueden estar grabando, ... Quiero decir. Las vulnerabilidades del sistema y, por lo tanto, cómo hacer esto… un sistema de puertos no tan universal, aunque por lo contrario es más incompatible…. Al final el mejor sistema de seguridad anti sistema o anti vulnerable por el sistema sería aquel que no hace servir el sistema, o se hace servir el sistema que no sean sistemas estándares, sino cajas cerradas que no se hablan con nadie. En el momento en que hasta incluso hay veces que a través de una máquina de vending que está en el sistema de red para saber si tienes stock o no tienes stock al final acabas entrando en el sistema tú no te esperabas que esta máquina de vending utilizará un puerto que fuera fácilmente accesible. Ahora bien, como lo tenemos que hacer al final? Cómo lo hacemos? Igual que nosotros hacemos los círculos concéntricos… la filosofía es la misma igual que tú tienes círculos concéntricos con la seguridad física y yo digo que a medida que me voy acercando voy cerrando el círculo aquí que tenemos que hacer?? Tenemos que hacer una evaluación de que lo que es nuestro cuore lo que nosotros queremos proteger. Por ejemplo, nóminas, sistemas de cámara, sistemas de señales ferroviarias …. Por decir algo. Por lo tanto, te tienes que poner de acuerdo con los diferentes usuarios de qué es lo que quieres proteger de ellos y a partir de aquí le pongo uno unos muros muy altos con los cortafuegos con los sistemas de control de sondas que me permiten ver si alguien me está penetrando …

Esa es la implementación que debe hacerlo sistemas y otra es el conocimiento en seguridad qué debe hacerlo el director de seguridad. Esta cosa que parece tan clara y que tú lo tienes tan clara parece que en el resto de empresas no lo tienen tan claro.

Somos operadores críticos y la ley 8/2011 te habla de la figura del CISO… nosotros somos los interlocutores, … ellos dependen funcionalmente de nosotros cuando creamos los planes de protección específicos que ellos hacen, …. Nosotros somos los que orgánicamente ... Y al final los que tenemos que gestionar todo esto.

La filosofía siempre también es la misma. Tú no coincidentes con el Olmos, ahora ya está jubilado y fue director general nuestro y trabajo junto conmigo desarrollando los materiales didácticos de la policía. Él tenía una frase que me hacía reír y en el fondo tenía razón. Decía que al final mandar es hacer. Y para hacer hace no hace falta que seas un experto en la materia; yo he mandado a la canina a los Tedax y a muchas especialidades de las cuales yo no tenía ni idea. Al final te digo una cosa, el último los últimos 5 años era jefe de un área básica policial y hacía mucho tiempo que ya no estudia unas diligencias. Yo sabría mucho más hacerlas a máquina que con el sistema el Sip que yo mismo creé.

Llega un momento que lo que tienes que tener claro es lo que tú bajo una filosofía de un jefe corporativo de seguridad, ... ¿Qué filosofía y al de atrás? Tú lo que tienes que hacer es configurar tu modelo de círculos concéntricos. Preguntas de cuál es tu cuore, por lo tanto, qué medidas tengo que poner en esto.

Se me cae un sistema lo que tengo que es detectar que me están intentando entrar entonces lo tengo que haber protegido muy bien, segundo poner sondas para ver si me están intentando entrar y tercera ser capaz de lo que se conoce como la resiliencia de volver a la situación en la que estaba antes de ser atacado.

Si tú esto lo tienes cubierto me falta ser ingeniero informático ni de telecomunicaciones, …

Resumiendo, primero evalúas, cuándo evaluar te salen amenazas y riesgos y a partir de estas amenazas y riesgos ¿qué haces? Haces los planes ya sean de contingencia de resiliencia etcétera. Los planes los haces en función de la gravedad del daño que te puedan hacer.

Al final insisto es un tema filosófico es exactamente lo mismo no hay ninguna diferencia. Te estoy hablando de los mismos conceptos, ...

6.- Hablemos ahora de Inteligencia. ¿Qué es para ti y cuál es su valor añadido??

Me encanta ABEL esta pregunta. Información no es inteligencia, ¿qué es inteligencia? Es el tratamiento de la información. El tratamiento de la información que te da un resultado predictivo normalmente, aunque también puede ser histórico

Si, pero el histórico también te da una predicción porque la historia es un ciclo

Es muy divertido porque cuando yo volví de Estados Unidos en el año noventa y cuatro me dice el conseller Pomesa oye he pensado en ti para que lleves la Unidad de Inteligencia……. Yo en esa época era criminólogo y después dice licenciatura… Tenía claro que teníamos que coger muchos datos y los teníamos que poder correlacionar para que te dieran una información. La investigación no es otra cosa que esto es coger datos y correlacionarlas. En el ámbito predictivo analítico, el análisis de la información que después te da un resultado más allá del tipo predictivo, lo que tienes que tener es una serie información histórica que te da unos resultados como bien has dicho tú que son de carácter cíclico. Por lo tanto, inteligencia es aquella capacidad de recoger datos útiles, …

Hoy en día tenemos el Big Data.

Al final se trata de datos útiles con correlación entre ellos qué te dan pronósticos de carácter inteligente. Para mí esto es la inteligencia.

¿Su valor añadido es el pronóstico que te da esta ventaja respecto al otro?

Bueno la prevención, pero también otras cosas, como preparación de estadios y nuevos escenarios. Al final lo que te permite es darte una perspectiva de carácter más comercial porque te permite estar al día de las necesidades que tendrán tales personas en el futuro.

Nosotros lo que tenemos que ver es hacia donde nos orientamos y lo podemos hacer correlacionando muchos datos, … tendencias migratorias, tendencias técnicas etcétera, …

Cuando hacemos un paso más es cuando interrelacionamos con caracteres externos como puede ser sociales, técnicos demográficos. ... Esto es lo que al final te permite hacer proyecciones.

Tengo una teoría, y es que, a través de la inteligencia, podemos obtener información que, hasta su llegada, la de la inteligencia, estaba sólo en manos de las FCSE. Se ha dado el caso en el que has recibido información mediante inteligencia mucho antes de recibirla por la vía tradicional (FCSE). En una sociedad denominada la sociedad de la información, donde quien tiene la información tiene el poder, si la parte privada dispone de más información porque

tiene más medios y por lo tanto tiene poder, ¿no crees que la relación entre la seguridad pública y privada se verá afectada y situará a la seguridad privada en una situación de ventaja, más allá de la complementariedad que determina la ley?, ¿ Crees que esta casuística va a cambiar la relación, no de Iure sino de facto, entre la seguridad privada y la seguridad pública?

Yo no diría esto disculpa. Yo lo que digo es que el sector público no tiene tantos recursos y por lo tanto el privado tiene más capacidad de crecimiento. Además, en los últimos años que no he ido oferta pública nos hemos dado cuenta que el sector privado tiene mucho más espacio del que tenía.

No acabo de estar de acuerdo. Yo creo que y sabes que yo no soy una persona… sí hace un momento he hablado de la coordinación, de colaboración, … creo que estás sobrevalorando la seguridad privada. Es verdad que tenemos agencias de inteligencia con estudios de BIGDATA, pero tienen limitaciones importantes me explico: ahí información es a las que no pueden llegar sobre todo por la normativa de protección de datos. En Estados Unidos es cierto que es un poquito más laxo y sigue podrían acceder a cierta información.

Yo te diría que las empresas de seguridad privada y de inteligencia nivel privado tienen limitaciones muy importantes y precisamente para evitar esto que dices tú precisamente. Y creo que lo sobrevaloras porque la seguridad privada … Cataluña por ejemplo en estos momentos tiene un déficit enorme de seguridad privada. Esto quiere decir que hay más demanda de seguridad privada que la oferta que hay.

En estos momentos en Barcelona hay más demanda que oferta por lo tanto cuando hablamos de seguridad privada estamos hablando unos perfiles que son lo que son, … aquí tenemos una gente una empresa que, de una gente muy buena, ... Pero al final hay empresas que no tienen el personal suficiente, … yo creo que es sobrevaloras la seguridad privada y que la seguridad privada, agencias de inteligencia de tratamiento de datos tienen unas limitaciones legales importantes, muy importantes y hasta incluso la seguridad pública también. Lo que pasa que la policía juega con los datos de elaboración propia en muchos casos. Por lo tanto, no te lo pierdas tú hablaste la seguridad privada como si fuera un ente. La seguridad privada está tremendamente diseminada, estamos hablando de muchas empresas, …. Por lo tanto, seguridad privada me parece un poco de ficción y casi de película pensar, actualmente, que están en situación de pasar la mano por la cara la seguridad pública. A mi modo de entender

están años luz esta situación. Es verdad la que la tendencia es que la seguridad privada irá creciendo más, … lo que pasa que al final cuando hablamos de inteligencia al final de que te sirve la inteligencia, ... Para uso propio o para venderla. Para venderla cuidado que esto tiene unas limitaciones terribles.

Y**o más que pensar en en empresas de seguridad está pensando en empresas como La Caixa o el Banco de Sabadell, ….**

¿A ver La Caixa qué trabaja? Ellos tienen un grupo de seguridad que trabajan información hacer una especie de inteligencia a través de tweet redes sociales, prensa, ... Ellos la información la correlacionan, es uno de los sitios más desarrollados que yo conozco, pero aun así es muy limitada y es de los más de los que yo conozco más potente, y todo y eso, es tremendamente limitada.

7.- Imagínate que eres el director de RRHH de una gran empresa y el CO te encarga contratar un DS. ¿Qué buscarías en DS?

Yo sé que para encontrarme a mí se tiraron 3 años y conozco a todos los que entrevistaron antes que a mí. La verdad mi honor Aarón mucho cuando pensaron en mí y sobre todo cuando existieron. Decir alguien como yo es tremendamente patán y engreído. Yo el día que falte o me jubile creo que buscaría un perfil parecido al mío. Parecido al mío quiere decir tal y como he comenzado la conversación…. Qué es lo que más se valora aquí? Que tengas muchos contactos es decir al final el director de seguridad es bueno en tanto en cuanto tiene muchos contactos y sabe exactamente a qué decirle esto, ... Y cómo has de analizar determinadas informaciones y como asesorar a la gente. La gente te pregunta oye me están haciendo esto me están extorsionando, … me han quitado la dirección de correo electrónico y están pidiendo dinero a la gente mi nombre, … o yo qué sé hay unos robos en una zona o están pasando droga por aquí o lo que sea. O quiero tener limpio mi despacho de posibles la paz. El hecho de que tengas todos los contactos para hacer esto con un chasquido de dedos para mí esto es muy fácil. Temas que para otro sería muy complicado para mí es muy fácil. Conocer a los interlocutores de la Guardia Urbana de los Mossos d'Esquadra de la Policía Nacional de la Guardia Civil por la por ejemplo por la problemática de robots en el Port Vell, … no es lo mismo que una persona que los tengan que cortar no venga de ningún cuerpo policial que una persona que ha sido comisario nuestros cuerpos y que además tiene un prestigio y conoce a este ya este. Esto facilita

enormemente las cosas. Yo no te digo que alguien no lo consiguiera, … aparte de esto evidentemente tiene que tener conocimientos yo muchas veces asesoró a la Policía Portuaria de muchas cosas que tienen que tener en cuenta, …

Sí tengo que ir a ver a la juez Degana no es lo mismo que vaya jefe de seguridad que un ex comisario.

Aparte de los conocimientos y perdona eh aparte hay una máxima y te la he comentado dos veces y ahora te la voy a volver a repetir. En definitiva, no se trata detener grande son muchos conocimientos. Se trata de tener una filosofía clara de lo que quieres hacer e implementar la. Para implementarla tienes que mover voluntades y para mover voluntades tienes que conocer políticas de recursos humanos y saber liderar las personas, ser un buen gestor de personas. Yo entiendo que si me cogieron es porque pensaron que ellos sería un buen gestor de recursos humanos sin perjuicio que además tenía tus valores que te he puesto encima de la mesa.

Hay una que se da en la parte pública y no sea la parte privada y es la jerarquía y es la jerarquía que tenemos autorizado a los policías que no tiene nada que ver con el sector privado.

Yo llegué aquí, llevaba muchos años en Mossos, tenía un prestigio, quiero pensar que todavía lo tengo porque no se pierde y por lo tanto mucha gente me discutía casi nada porque yo tenía la auctoritas. Yo cuando llegué aquí me tuve que ganar está autorcitas, los sindicatos me llamaban El Mesías porque me esperaban. Cuando llegué aquí y vieron que el Mesías no camina no camina por las aguas del mar y vieron que el Mesías era una persona normal y que además se ajustaba a las políticas de la alta dirección. Yo formo parte del comité dirección de esta casa cosa que antes cuando llegue no formaba parte y por lo tanto al principio tuve que pasar por un proceso como si viniese de la calle por mucho que tuviera una aureola porvenir de Mossos y ser comisario. Yo comencé no de 0 pero sí de muy abajo. El prestigio que tenía en mosos me lo he tenido que ganar aquí picando piedra.

Poco a poco recuperar la credibilidad y si encima tienes técnica y habilidades para gestionar recursos humanos pues se forma un cóctel: conocimientos técnicos conocimientos de gestión de personas y credibilidad y honestidad, acabaste en el perfil necesario para ser director de seguridad.

6.- Una de las funciones que no dice la ley que tiene que tener un director de seguridad que no le atribuye la ley, pero quizás sea la más importante y sobre todo en un espacio donde en

la ciberseguridad el usuario es la principal amenaza es lo que conocemos como cultura de seguridad. Me gustaría saber cómo percibes tú esto.

Bien entrada usted todo el rato haces referencia a la Ley de Seguridad Privada que en breve tendrá su reglamento, pero es que nosotros y quiero que entiendas dos cosas, ... Y tal vez lo tenía que haber puesto esto por delante.

Yo me rijo más por seguridad pública que por seguridad privada me explico: aquí la seguridad ... Privada el puerto prácticamente no tiene. Un parking que tiene unos vigilantes y unos accesos que ya hemos pasado a terceros así que ni eso. Te decía hace un momento la posibilidad de externalizar el control de accesos. Nosotros no tenemos seguridad privada quién tiene seguridad privada son las empresas que trabajan en el puerto que dependen a nivel de seguridad. Quién les dice si tiene los niveles de seguridad adecuados o no es la figura del oficial de seguridad portuaria que este señor depende de mí y dice que está estación cumple o no cumple los requisitos de seguridad.

Por lo tanto, nosotros somos seguridad pública incluso la Policía Portuaria depende de Fomento y Puertos del Estado. Por lo tanto, somos seguridad pública. Yo no tengo una visión de seguridad privada y te digo esto… y sí que es verdad que en mis tarjetas pone que soy director de Seguridad Corporativa, pero por ejemplo la ley que antes hemos hecho referencia, sí que habla de que la seguridad se impregna en todos los sistemas, que hemos de tomar medidas para qué la política y por lo tanto la filosofía de seguridad dentro de este modelo de sistema donde todo el mundo acaba configurando el sistema, … es decir, yo tengo que demostrar hechos y actos y reuniones qué yo explico las políticas de seguridad en el Comité de Dirección y hasta el consejo de administración. Yo las explico y porqué dentro del plan de seguridad, el plan operativo de seguridad del puerto, … por qué protegemos esto?

Igual que antes te he dicho que en el ámbito informático tenemos que proteger lo que es cuore en el ámbito físico o en el ámbito global que es todo yo tengo que decir porqué proteger determinado activo, ...

Entonces esto yo lo tengo que explicar y además después lo tengo que hacer llegar abajo. De alguna manera las políticas de seguridad de la casa se tienen que explicar hacia arriba y hacia abajo y no sólo esto, también de la mano de sistemas, ...