



GUÍA SOBRE SEGURIDAD E INTELIGENCIA ESTRATÉGICA PARA PYMES

Una guía que orienta sobre la necesidad de la inteligencia y seguridad en los procesos de internacionalización de las pymes

GUÍA SOBRE SEGURIDAD E INTELIGENCIA ESTRATÉGICA PARA PYMES

Una guía que orienta sobre la necesidad de la inteligencia y seguridad en los procesos de internacionalización de las pymes

Diciembre 2020

DIRECCIÓN

Jesús de Miguel. SOCIO TWO WORLDS COLLABORATIVE INTELLIGENCE (TWCI)

Salvador Marín. PRESIDENTE EFAA FOR SMEs Y DIRECTOR CÁTEDRA EC-CGE

Raúl Mínguez. DIRECTOR SERVICIO DE ESTUDIOS CÁMARA DE COMERCIO DE ESPAÑA

EQUIPO DE TRABAJO

Carlos Blanco. SOCIO TWO WORLDS COLLABORATIVE INTELLIGENCE (TWCI)

Pedro Cid. SOCIO TWO WORLDS COLLABORATIVE INTELLIGENCE (TWCI)

Jesús de Miguel. SOCIO TWO WORLDS COLLABORATIVE INTELLIGENCE (TWCI)

Salvador Marín. PRESIDENTE EFAA FOR SMEs Y DIRECTOR CÁTEDRA EC-CGE

Francisco Javier Martínez. VICEPRESIDENTE EC-CGE Y UNIVERSIDAD DE CANTABRIA

Esther Ortiz. MIEMBRO CONSEJO DIRECTIVO EC-CGE Y UNIVERSIDAD DE MURCIA

Carolina Perondi. ANALISTA SERVICIO DE ESTUDIOS CÁMARA DE COMERCIO DE ESPAÑA

La competitividad empresarial es un concepto complejo y dinámico, reflejo de la capacidad de producir bienes y servicios en un mercado integrado en la economía mundial de un modo tal que permita el crecimiento sostenido de la productividad y de los ingresos. La mejora de la competitividad de toda empresa debería ser el núcleo vertebrador de su estrategia y operativa empresarial.

Detrás del concepto de competitividad se distinguen dos bloques de factores. Por una parte, las cuestiones de carácter microeconómico o empresarial, aquellos aspectos caracterizados por la capacidad de la empresa para incidir sobre los mismos (estrategia, diseño, reputación, innovación, gestión de los recursos humanos, etc.). A éstos se suman determinados factores del entorno externo de las empresas que influyen sobre la competitividad empresarial, como las infraestructuras (transporte, comunicaciones, energéticas), la calidad institucional o el marco regulatorio de la actividad económico-empresarial, entre otros.

Un factor clave y de relevancia creciente en el ámbito de la competitividad interna, empresarial o microeconómica, lo constituye la decisión y habilidad para articular una inteligencia empresarial o competitiva propia. Esto es, ser capaz de aglutinar información relevante, aplicar las técnicas de análisis adecuadas, y extraer un conocimiento que, aplicado a la toma de decisiones, ofrezca una inteligencia que contribuya a asegurar las operaciones y la continuidad y competitividad del negocio.

De este modo, la inteligencia aplicada al ámbito empresarial es un factor clave para la seguridad de la compañía y un refuerzo de la capacidad de la empresa para mejorar el proceso de toma de decisiones y garantizar el progreso futuro de la compañía.

Estas evidencias aún son desconocidas o no aplicadas por una parte relevante de nuestro tejido empresarial, especialmente pequeñas y medianas empresas. Por ello, el Consejo General de Economistas de España y la Cámara de Comercio de España, con la colaboración adicional de Two Worlds Collaborative Intelligence, hemos elaborado y editado una guía capaz de orientar sobre la necesidad de la inteligencia y seguridad en los procesos de internacionalización de las pymes.

El equipo de trabajo, conformado por reconocidos especialistas en las diferentes materias abordadas y dirigido por **Jesús de Miguel**, **Salvador Marín** y **Raúl Mínguez**, ha preparado un documento de referencia para comprender el contenido y relevancia de los conceptos de inteligencia y seguridad aplicados al mundo empresarial, su interrelación, y analizar la posible evolución del actual escenario geoestratégico, marcado por la pandemia del COVID-19. Además, se proporcionan criterios para evaluar el grado de conocimiento y aplicación de estos conceptos en las empresas, describiéndose las diferentes soluciones de seguridad e inteligencia estratégica internacional existentes para las pymes.

En suma, una completa guía para ayudar a las pymes a consolidar su negocio y sentar las bases para su expansión exterior, especialmente relevante en momentos de incertidumbre como los actuales.

Debemos agradecer la minuciosa labor del equipo participante en esta guía, así como el apoyo al proyecto por parte de **Inmaculada Riera**, Directora General de la Cámara de Comercio de España, y **Andrés Pereda**, Director de Desarrollo Corporativo de dicha institución.

Con esta publicación, queremos manifestar nuestro firme compromiso con el tejido productivo de nuestro país, con su internacionalización y con su capacidad para afrontar el presente desafío derivado de la crisis sanitaria y sus consecuencias económicas y sociales.

José Luis Bonet

PRESIDENTE
CÁMARA DE COMERCIO DE ESPAÑA

Valentín Pich

PRESIDENTE
CONSEJO GENERAL DE ECONOMISTAS DE ESPAÑA

INTRODUCCIÓN. ¿POR QUÉ UNA GUÍA DE SEGURIDAD E INTELIGENCIA ESTRATÉGICA PARA LAS PYMES?	09
REVISIÓN DE LA LITERATURA O ESTADO DEL “ARTE”	12
Evolución del concepto de inteligencia competitiva	12
Situación de la inteligencia competitiva en el mundo	17
La inteligencia competitiva en España	18
BREVE ANÁLISIS Y POSIBLE EVOLUCIÓN DEL NUEVO ESCENARIO GEOESTRATÉGICO	19
El complejo escenario económico en España tras la COVID-19	21
EL CONCEPTO DE SEGURIDAD AMPLIADA APLICADO A LAS EMPRESAS	24
EL MERCADO DE LA INTELIGENCIA. UN MERCADO EN EXPANSIÓN EN LA INTERNACIONALIZACIÓN EMPRESARIAL	28
LA APLICACIÓN DE LA INTELIGENCIA PARA LA SEGURIDAD EN LAS PYMES. ¿ES TU NEGOCIO SEGURO?	32
La inteligencia como herramienta proactiva	35
LA INTELIGENCIA COMPETITIVA. ¿ES TU NEGOCIO COMPETITIVO?	38
EL MODELO DE INTELIGENCIA COLABORATIVA EN EL NUEVO ENTORNO ESTRATÉGICO MUNDIAL	45
SOLUCIONES DE SEGURIDAD E INTELIGENCIA ESTRATÉGICA INTERNACIONAL PARA LAS PYMES. BUENAS PRÁCTICAS	48
A MODO DE SÍNTESIS	61
ACRÓNIMOS	65
BIBLIOGRAFÍA	66

INTRODUCCIÓN ¿POR QUÉ UNA GUÍA DE SEGURIDAD E INTELIGENCIA PARA LAS PYMES?

A mayor nivel de incertidumbre más necesaria se hace la inteligencia para cualquier organización, ya sea pública o privada.

Las empresas de cualquier tamaño y dimensión, especialmente aquellas que están empezando un proceso de internacionalización o se encuentran ya internacionalizadas, precisan un conocimiento lo más detallado posible del entorno en el que desarrollan su negocio. Se habla de la necesidad de tener una superioridad informativa, pero este término, sin más, no refleja la amplitud del concepto de inteligencia.

“The power to question is the basis of all human progress”

Indira Gandhi

Hoy en día, gracias al impresionante desarrollo tecnológico, disponemos de un gran volumen de información que por sí mismo no representa ningún valor añadido. La superioridad informativa la debemos entender como la disponibilidad en tiempo oportuno y de forma precisa de la información debidamente tratada y analizada, es decir de la inteligencia. Solamente de esta manera se alcanzará la verdadera ventaja competitiva.

ILUSTRACIÓN 1. INTELIGENCIA ESTRATÉGICA



Fuente: <https://images.app.goo.gl/9JGsCiGM6jUZhYnw8>

La inteligencia de la que hablamos tiene dos grandes componentes, el estratégico, orientado a la toma de decisiones, y la inteligencia operacional y táctica, orientadas a preservar el día a día de la operación, la continuidad de negocio, todo ello en el marco de la inteligencia competitiva, que más adelante desarrollaremos (*las interconexiones entre inteligencia y estrategia se ponen de manifiesto en la ilustración 1*). En este campo serán varios los aspectos a valorar. Desde la seguridad física de personas, infraestructuras, o activos, entre otros, como los de la seguridad lógica frente

a las ciber amenazas, o la propia seguridad económica de la operación. Como vemos, inteligencia y seguridad, se encuentran íntimamente relacionadas. Cuando hablamos de seguridad se debe tomar en consideración una idea clave: su finalidad última es la supervivencia de la organización y, por tanto, es un elemento fundamental de la cadena de valor de cualquier

empresa, con independencia de su tamaño, siendo precisamente la inteligencia una herramienta fundamental para garantizar esta seguridad.

Es importante también avanzar en esta introducción que cuando hablamos de seguridad, lo hacemos en un concepto mucho más amplio que el tradicional, nos referimos a una *seguridad ampliada* o lo que llamamos una **seguridad de 360°**. Al abordarla desde esta perspectiva observamos su carácter multidimensional, que incluye los aspectos humanos, medioambientales, nacionales, económicos, o sociales, entre otros. También entendemos que esta visión amplia debe ser enfocada de una manera integral, lo que quiere decir que compete a toda la organización, con independencia de que la responsabilidad de su dirección se encuentre al más alto nivel directivo. Es pues una función transversal, y que en consecuencia afecta a todos los departamentos de la organización y debe ser dirigida al más alto nivel. Por último, hablamos de que la seguridad tiene una clara dimensión global, al estar afectada por riesgos y amenazas que tienen su origen fuera de los ámbitos fronterizos de cualquier país, como así quedó patente en la crisis económica del 2008 y más evidente, aún si cabe, en esta reciente crisis de la COVID-19.

El objetivo de esta guía es precisamente concienciar al sector empresarial y otras organizaciones, en particular a los propietarios, gerentes y directivos de las pequeñas y medianas empresas, de la importancia que tiene incorporar la inteligencia a los procesos de sus organizaciones. Su incorporación a los procesos internos de las empresas no significa que éstas se vean obligadas a organizar su propio departamento de inteligencia, esto es algo que solamente las empresas de mayor dimensión organizativa suelen asumir, por el mayor coste económico que supone, pero sí que deben dotarse de ella. Por otra parte, existe una tendencia cada vez más generalizada en el mundo empresarial, incluso en muchas instituciones, a concentrar el esfuerzo económico y organizacional en el *core* de dicha organización, recurriendo a fórmulas de *outsourcing* para diseñar y desarrollar los procesos que no tienen una relación directa con la actividad de la empresa, siendo la inteligencia uno de ellos, por su carácter altamente especializado.

No obstante, esto no quiere decir que la inteligencia no sea una actividad fundamental o *core*, sino que para muchas empresas –y unas de ellas son las pymes– es un servicio que se deberá externalizar o contratar como parte integral de su actividad empresarial. En este sentido, hay que tener también en cuenta el amplio campo que, como ya se apuntaba, abarca la función de inteligencia, lo que exigiría tener una infraestructura sobredimensionada, que redundaría en unos costes inasumibles. Por este motivo, y facilitado por el amplio desarrollo tecnológico, la mayoría de las compañías y/o profesionales que ofrecen este tipo de servicios, lo hacen en el ámbito de lo que se conoce como **Inteligencia Colaborativa**, de la que también hablaremos en esta guía, concepto que de una manera muy simplista podríamos definir como la posibilidad de elegir la mejor opción para alcanzar una determinada meta trabajando en

conjunto para preservar la seguridad y la competitividad de cualquier organización. Ésta se basaría en el establecimiento de una red de contactos y un conocimiento compartido en diferentes actividades, apoyado por la implantación de herramientas inteligentes (2.0) y basado en la cooperación y en la confianza mutua.

Pretendemos con ello aprender cómo acceder a la totalidad de la única inteligencia que se encuentra con nosotros y entre nosotros. Para ser competitivo en una economía global debemos aprender a pensar y actuar de manera innovadora y colaborativa. El principio clave de una inteligencia colaborativa:

Cuanto más compartamos más tendremos

Jesús de Miguel
Socio TWCI

Salvador Marín
Presidente EFAA for SMEs

Raúl Mínguez
Director Servicio Estudios
Cámara Comercio de España

REVISIÓN DE LA LITERATURA O ESTADO DEL "ARTE"

EVOLUCIÓN DEL CONCEPTO DE INTELIGENCIA COMPETITIVA

El concepto de Inteligencia competitiva (IC) y su consideración como disciplina, desde sus inicios hasta la actualidad, ha estado en constante evolución condicionado por el contexto, la tecnología disponible, y las necesidades detectadas por las organizaciones.

Si bien en sus inicios la IC surge como una herramienta de marketing, centrada en clientes y competidores; tiene su origen en la inteligencia militar, económica, comercial y política. A partir de ahí, la disciplina ha ido evolucionando hasta integrar aspectos más estratégicos y abarcando toda la cadena de valor.

Y en este marco, la IC ha sido, y aún continúa siéndolo, definida de múltiples formas y a través de diferentes terminologías, atendiendo a los procesos que engloba y a las prioridades atribuidas según las necesidades de información.

Esta falta de unanimidad a la hora de definirla, y de terminología común, es consecuencia de las múltiples disciplinas que la conforman, cuya relevancia y peso varían en función del objetivo perseguido y del ámbito desde el que se aborda. Se han utilizado muchos adjetivos para acompañar el término "inteligencia", atendiendo en la mayoría de los casos a las diferentes disciplinas desde las cuales se aborda el conocimiento. Sirvan como ejemplo inteligencia tecnológica, inteligencia económica, inteligencia competitiva o inteligencia de mercado, entre otros.

En esta línea, Cavaller (2009) menciona algunos de los términos sinónimos o complementarios de la IC más comunes en inglés, destacando *competitive intelligence*, *business intelligence*, *competitor intelligence*, y *environmental scanning*, añadiendo la forma francesa *Intelligence économique*, e *Inteligencia tecnológica*, limitada esta última al ámbito tecnológico.

Cavaller (2009) realiza también un compendio de las definiciones de inteligencia competitiva y sus formas derivadas, 26 en total, que considera más significativas y que ilustran cómo ha evolucionado el concepto entre los años 1980 y 2003 (estas definiciones se recogen en la tabla 1). Destaca que, a mediados de los ochenta, la definición de IC de Shrivastava y Grant era "sistema de aprendizaje sobre las capacidades y comportamientos de los competidores actuales y potenciales con objeto de ayudar a los responsables en la toma de decisiones estratégicas". Unos años después, Gilad (1992) la define como "el acceso a tiempo al conocimiento e información relevantes en las diferentes fases de la toma de decisiones". Diez años más tarde, para Bergeron y Hiller (2002) la IC es "la recogida, la transmisión, el análisis y la difusión de la información relevante públicamente disponible, ética y legalmente obtenida como medio para la producción de conocimiento procesable para la mejora de la toma de decisiones y acciones corporativas".

Cavaller (2009) finaliza el compendio con una definición propia, según la cual *“La inteligencia competitiva es la gestión sistemática de la información orientada estratégicamente al progreso de las organizaciones. Incorpora las tres dimensiones fundamentales procesuales: sistema - información - estrategia, que constituyen la condición necesaria para elevar una actividad organizativa al modo de la inteligencia. Integra en orden de aplicación las siguientes seis tipologías de vigilancia: del entorno, organizativa, competitiva, económica, tecnológica, estratégica.”*

TABLA 1. DEFINICIONES DE INTELIGENCIA COMPETITIVA (IC) Y FORMAS DERIVADAS

ND	AUTOR	AÑO	TI	DEFINICIÓN
1	Aguilar	1967	ES	La exploración del entorno (Environmental scanning) es la adquisición y el uso de la información sobre acontecimientos, tendencias y relaciones en el entorno externo de una organización, cuyo conocimiento asistirá a la gerencia a planear la organización una línea de conducta futura.
2	Porter	1980	CI	El objetivo de la inteligencia del competidor (<i>Competitor Intelligence=CI</i>) es desarrollar una representación de la naturaleza de los cambios probables de la estrategia que cada competidor puede realizar, la respuesta probable de cada competidor a los movimientos estratégicos de la competencia y la reacción probable de cada competidor a los cambios de la industria y del entorno. La CI se centra en las acciones, los comportamientos y las opciones por el hecho de existir unos o más competidores potenciales.
3	Berenguer	1982	BI	Las unidades de inteligencia empresariales (<i>Business intelligence</i>) son pequeños órganos funcionales interdependientes, que recogen información interna y externa de la empresa, la tratan intelectualmente y la difunden a las restantes unidades funcionales y a los distintos niveles jerárquicos de la empresa.
4	Shrivastava y Grant	1985	IC	La IC es el sistema de aprendizaje sobre las capacidades y comportamientos de los competidores actuales y potenciales con objeto de ayudar a los responsables en la toma de decisiones estratégicas.
5	Sutton	1988	IC	La IC se refiere al análisis de competidores así como a las condiciones competitivas en las industrias o las regiones particulares.
6	SCIP	1988	IC	La IC es el proceso de supervisar el ambiente competitivo que permite a los directivos de las empresas de todos los tamaños tomar las decisiones informadas sobre todo en el relativo a la comercialización, I+D, y de invertir tácticamente en estrategias de negocio a largo plazo.
7	Gilad i Gilad	1988	BI/IC	La inteligencia empresarial (<i>Business intelligence</i>) se ha descrito como la actividad de supervisar el ambiente externo de la empresa para obtener la información que es relevante para el procedimiento de toma de decisiones. En la práctica, la BI se concentra a menudo en competidores actuales como en la IC, pero también puede incluir áreas como el análisis de adquisiciones, de fusiones potenciales y de los gravámenes de riesgo en los países.

ND	AUTOR	AÑO	TI	DEFINICIÓN
8	Baumard	1991	IE	La inteligencia económica no es sólo observación sino una práctica ofensiva y defensiva de la información. Su objetivo consiste al relacionar diversas áreas para servir a los objetivos tácticos y estratégicos de la empresa. Es una herramienta que conecta el saber de la empresa con la acción.
9	Gilad	1992	IC	La IC es el acceso a tiempo al conocimiento e información relevantes en las diferentes fases de la toma de decisiones.
10	Kokubo	1992	IT	La inteligencia tecnológica para la I+D consiste fundamentalmente en la recogida de información técnica, la distribución de la información adquirida a las personas correctas y el trabajo analítico para el proceso de decisión.
11	Choo y Auster	1993	ES	La exploración del entorno (<i>Environmental scanning</i>) es la adquisición y el uso de la información sobre acontecimientos, tendencias y relaciones en el entorno externo de una organización, cuyo conocimiento asistirá a la gerencia a planear la organización una línea de conducta futura. / Las organizaciones exploran el ambiente en orden a entender fuerzas externas del cambio con el fin de desarrollar las respuestas eficaces para mejorar la propia posición en el futuro. / La exploración cubre no sólo a competidores, proveedores y clientes sino que también incluye tecnología, las condiciones económicas, el ambiente político y las tendencias sociales y demográficas.
12	Choo	1998a		
13	Heiser	1994	IT	La inteligencia tecnológica consiste en el seguimiento o exploración y análisis estratégico del progreso de la ciencia y la tecnología. No se trata de obtener información y hacer informes sino de dar apoyo a las organizaciones en la gestión de la tecnología para que tomen decisiones correctas en el tiempo adecuado.
14	Martre	1994	IE	La Inteligencia económica (IE) integra los resultados de la vigilancia en diferentes ámbitos: científico y tecnológico, competencial, financiero, jurídico y reglamentario.
15	Rouach	1996		
16	Degoul	2000		
17	Groupe de Projet Intelligence Economique	1995	IE	La inteligencia económica está constituida por el conjunto de conceptos, instrumentos, metodologías y prácticas que permiten poner en relación de manera pertinente diferentes conocimientos e informaciones en la perspectiva del dominio y de los desarrollo de la dinámica económica. Esta puesta en relación implica en particular: una movilización humana, un tratamiento y análisis de la información y del conocimiento orientados hacia una finalidad operacional, una circulación eficaz de las informaciones y de los conocimientos en el seno de las organizaciones implicadas.
18	Ashton i Stacey	1995	IT	La inteligencia tecnológica es el proceso de investigación, análisis y uso de la mejor información sobre desarrollos, hechos y tendencias en el entorno científico y tecnológico.
19	Ettorre	1995	IC	La IC es el proceso mediante el cual las organizaciones obtienen informaciones útiles sobre sus competidores que utilizan en sus planificaciones a corto y largo plazo.
20	Gibbons i Prescott	1996	IC	La IC es el proceso de obtención, análisis, interpretación y difusión de información de valor estratégico sobre la industria y los competidores, que se transmite a los responsables de la toma de decisiones en el momento oportuno.

ND	AUTOR	AÑO	TI	DEFINICIÓN
21	Ashton i Klavans	1997	IT	La inteligencia tecnológica es la investigación, detección, análisis y comunicación a los directivos de la empresa de informaciones orientadas a la toma de decisiones sobre oportunidades, amenazas, tendencias o desarrollos exteriores en el ámbito de la ciencia y la tecnología que pueden afectar a la situación competitiva de la empresa.
22	Cottril	1998	IC	La IC es la obtención ética y legal, análisis y distribución de información sobre el entorno competitivo, incluyendo los puntos fuertes y débiles así como las intenciones de los competidores.
23	Rodríguez	1999	IC	La inteligencia se diferencia de la vigilancia en el hecho de que no se limita a la simple obtención de información sino que pone énfasis en la selección de esta información, en su análisis y en su presentación de forma adecuada para que los directivos puedan tomar las decisiones. (...) La inteligencia presenta una información más elaborada y mejor preparada para la toma de decisiones.
24	Nordey	1999	IE	La vigilancia tecnológica contribuye a la inteligencia económica, pero no es suficiente para completar la inteligencia económica. La inteligencia integra a la vez: la documentación, la vigilancia documental, las vigilancias especializadas (o sectoriales) y la vigilancia estratégica.
25	Bergeron i Hiller	2002	IC	La IC es la recogida, la transmisión, el análisis y la difusión de la información relevante públicamente disponible, éticamente y legalmente obtenida como medio para la producción de conocimiento procesable para la mejora de la toma de decisiones y acciones corporativas.
26	Cavaller	2003	IES	La inteligencia estratégica es la gestión sistemática de la información orientada estratégicamente al progreso de las organizaciones. Incorpora las tres dimensiones fundamentales procesuales: sistema - información - estrategia, que constituyen la condición necesaria para elevar una actividad organizativa al modo de la inteligencia. Integra en orden de aplicación las siguientes seis tipologías de vigilancia: del entorno, organizativa, competitiva, económica, tecnológica, estratégica.

Fuente: Cavaller (2009, p. 36-38)

Las definiciones recopiladas por Cavaller (2009) ponen de manifiesto los cambios experimentados por la disciplina a lo largo de los años, hacia una visión más estratégica de su cometido. En esta misma línea, destaca también el trabajo de Prescott (1999), en el que profundiza en las etapas evolutivas de la IC, resaltando la incorporación creciente de un enfoque cada vez más estratégico, al tiempo que incide en el análisis e introduce la IC como una herramienta clave en las instancias directivas (*ver tabla 2, página siguiente*).

Así, en las definiciones más recientes de IC, subyace su objetivo estratégico. En esta línea, Gilad (2015) presenta una sencilla y clara definición: *“IC es una perspectiva sobre la evolución de las condiciones del mercado. Esto significa identificar riesgos y oportunidades lo suficien-*

TABLA 2. EVOLUCIÓN DE LA INTELIGENCIA COMPETITIVA

PERIODO	PRE-1980	1980-1987	1988-PRESENTE	FUTURO
Estados	Toma de Datos de la Competencia	Análisis Industrial y competidor Análisis	Inteligencia Competitiva	Inteligencia Competitiva como una esencial capacidad
Evento	Porter (1980) con su libro Estrategia Competitiva	Fundación de la SCIP	La aceptación de la revista <i>Competitive Intelligence Review</i>	IC cursos en escuelas de negocios
ATRIBUTOS				
Grado de Formalidad	Informal	Emergen Unidades Formales	Formal	Integración de Formal a Informales
Orientación	Táctica	Táctica	Mixta	Estratégica
Análisis	Pequeño o nada	Limitado y cuantitativo	Cuantitativo y cualitativo	Énfasis cualitativo
Atención de Top Management	Bajo	Limitado	Moderado	Alto
Vínculo con los Procesos de Toma de Decisiones	Pequeño	Débil	Fuerte	Directo
LOCALIZACIÓN				
Principal Localización del personal de IC	Bibliotecas/ Marketing	Planeación/ Marketing	Planeación/ Marketing / UIC	UIC / Planeación /Marketing
PROBLEMAS				
	Desarrollo de habilidades en adquirir información	Construir un caso de IC, Imagen de espía, Desarrollo de habilidades analíticas	Demanda y oferta de IC, Contrainteligencia: Inteligencia, IC Tecnológica, Rol de la información Tecnológica	Administrar en paralelo los procesos de inteligencia de multinacionales, IC es aprendizaje

Fuente: BAI (2008)

temente pronto como para permitir a la empresa adaptar su estrategia o, en casos extremos, cambiarla."

Sánchez (2015), por su parte, define a la inteligencia, aplicada al campo económico o empresarial, como *"una herramienta enfocada a administrar y generar el conocimiento necesario, tanto para satisfacer las necesidades de información que demanda la alta dirección para una acertada toma de decisiones, como para anticiparse a potenciales situaciones críticas futuras."*

En términos más operativos, la Agencia de Innovación de Bizkaia (BAI, 2008), citando a Bill Gates, en el libro *Business @ the Speed of Thought*, resume las ventajas que para una empresa representa contar la IC: *"cómo recolectamos y manejamos la información determinará las pérdidas o ganancias. Ahora hay más competidores, hay más información disponible sobre ellos y sobre el mercado, que es global. Los ganadores serán los que desarrollan un sistema de inteligencia, de modo que la información y el conocimiento puedan atravesar fácilmente sus compañías para que aprendan constantemente."*

En definitiva, a pesar de la falta de consenso para una definición común de Inteligencia competitiva, sí parece existir cierto acuerdo en cuanto a su finalidad y los procesos que engloba en la práctica.

SITUACIÓN DE LA INTELIGENCIA COMPETITIVA EN EL MUNDO

La evidencia indica que son las empresas de las economías más desarrolladas las que apuestan con mayor decisión por la inteligencia competitiva. No existe un modelo global de inteligencia, sino distintos sistemas que responden a las particularidades de cada país, según las conclusiones alcanzadas por la Agencia de Innovación de Bizkaia (BAI, 2008).

Las prácticas de inteligencia vinculadas a los negocios vienen desarrollándose desde hace siglos, tanto desde el sector público como desde el privado. Sin embargo, no es hasta 1986, con la creación de la *Society of Competitive Intelligence Professionals* (SCIP) en EE.UU, cuando se inicia el camino hacia su reconocimiento formal como una disciplina (BAI, 2008).

Desde el sector público, las prácticas se iniciaron en el marco de la inteligencia militar y evolucionaron a la inteligencia económica, en la búsqueda de ventajas competitivas en mercados cada vez más globalizados. En las empresas, surgieron con el objetivo de ganancia competitiva.

En cuanto a la implantación en los distintos países, su grado de desarrollo es heterogéneo, debido a la influencia de factores tales como la cultura-país, la necesidad de competir ante una escasez de determinados recursos o a la crisis económica, y el entorno empresarial (Izquierdo, 2018).

Países como Japón, Corea del Sur, Suecia, Canadá, Reino Unido, Israel y EE. UU son referentes en este campo, siendo de los más activos en materia de IC. Así, por ejemplo, Japón es considerado el país pionero en IC desde la finalización de la segunda guerra mundial, seguido por EE. UU. Suecia es reconocida internacionalmente por sus programas en la materia, en tanto que Francia lidera el desarrollo de programas informáticos para la elaboración de mapas tecnológicos (BAI, 2008).

El enfoque desarrollado por cada país para su implantación también varía. Durante siglos, las grandes potencias económicas han creado estructuras para el desarrollo de la IC, siendo

los enfoques diferentes, según desde qué instancias se impulsa su implantación. Así, han surgido tres modelos mayoritarios, el promovido desde el sector público hacia el privado (*top-down*), por iniciativa de las empresas (*bottom-up*) o de manera mixta, en colaboración público-privada.

De este modo, surgen estructuras de integración entre los principales grupos de interés, como son los servicios públicos, las asociaciones empresariales, las universidades, los sindicatos o la diáspora de expatriados. Concretamente, países como Francia, Japón o Corea del Sur se han desarrollado desde un enfoque *top-down*. EE. UU, Suecia y Reino Unido han utilizado la dinámica *bottom-up*. Finalmente, Canadá e Israel presentan un sistema mixto entre lo público y lo privado (MESIAS, 2018).

LA INTELIGENCIA COMPETITIVA EN ESPAÑA

El estudio de la IC como disciplina se inicia en España en los años 90 del siglo XX. Desde entonces comienza su intento de desarrollo, fase en la que se encuentra actualmente (Izquierdo, 2019). A este respecto, García Alsina (2011) menciona que en los 90 existían ya iniciativas caracterizadas por la obtención de información sobre el mercado, los competidores y la tecnología, y es a partir del año 2000 cuando las prácticas comienzan a estar más relacionadas con la estrategia de la organización.

ILUSTRACIÓN 2. FASES DE EVOLUCIÓN EN EL CONCEPTO DE IC EN ESPAÑA



Fuente: Izquierdo (2019)

Según señala MESIAS (2018), en España el monopolio de la inteligencia económica ha recaído en el Estado, centrado fundamentalmente en la lucha antiterrorista. En los últimos años, de la mano de la internacionalización, el tejido empresarial español está promoviendo su utilización, con múltiples compañías que ofrecen servicios de inteligencia.

En esta línea, Izquierdo (2019) señala que la implantación de la IC en el tejido productivo español, si bien está en crecimiento desde 2005, continúa siendo inferior a la de los países de nuestro entorno y es desarrollada exclusivamente por las grandes empresas, por lo que queda mucho recorrido y necesidad real –por su utilidad y fuente de ventaja competitiva– en las pymes (las diferentes fases en la evolución del concepto se incluyen en la ilustración 2).

BREVE ANÁLISIS Y POSIBLE EVOLUCIÓN DEL NUEVO ESCENARIO GEOESTRATÉGICO

La pandemia del COVID-19 no puede ser considerada propiamente como el factor originador del cambio, por cuanto éste estaba ya iniciado desde hace unos años, sino más bien como su catalizador. De una manera breve, cabría analizar el cambio que sin duda va a suponer bajo las siguientes cuatro grandes perspectivas: las geopolíticas, las económicas, las derivadas de la globalización digital, y las relacionadas con el individuo y la sociedad.

ILUSTRACIÓN 3. MAPAMUNDI



Fuente: <https://www.gettyimages.es>

GEOPOLÍTICAS

El factor más importante para tener en cuenta desde un punto de vista geopolítico para las empresas es la falta de liderazgo mundial en la época del "postcovid", a diferencia de otras etapas históricas.

Estados Unidos, en particular desde la llegada de Trump a la Casa Blanca, ha modificado su papel de líder global. Trump desde su visión *America first* ha lanzado este mensaje al mundo, y lo ha puesto de manifiesto en esta crisis. Por otra parte, la poderosa América de finales del pasado siglo desapareció, Estados Unidos sigue siendo el principal poder geopolítico, pero ya no lo es tanto en la agenda económica y mucho menos si hablamos de su influencia cultural.

China no descarta asumir ese papel, de hecho, aspira a ejercer un liderazgo global, como lo demuestra la expansión de su poder militar, especialmente naval; las ayudas al desarrollo para ir construyendo una red de influencia, mediante la aplicación del poder blando, que definiría Joseph Nye; su crecimiento económico, aunque actualmente más contenido por el coronavirus; y su desarrollo tecnológico, especialmente en el campo de las telecomunicaciones. Es innegable la creciente expansión de China en África y en buena parte de Latinoamérica, por lo que es de prever que en los próximos años tenga una influencia creciente en los mercados, de una manera muy particular en algunas áreas del planeta.

*“Un Mundo sin liderazgo global.
Mayor importancia de lo regional”*

Finalmente, la **Unión Europea** se encuentra sumida en una renovación de su identidad, resaltada con la salida del Reino Unido. Se puede simplificar diciendo que actualmente está inmersa en una pugna entre el norte y el sur, entre el este y el oeste o entre el nacionalismo y la integración. Antes de la llegada del coronavirus, Europa estaba ya tratando de adaptarse a esta nueva situación, intentando no ceder protagonismo y liderazgo en la escena internacional (*Ilustración 3*).

ECONÓMICAS

Son diferentes los aspectos a analizar en este campo; de momento, el impacto en el crecimiento económico a nivel global, que se estima tendrá, según previsiones del FMI (mayo 2020) y del Informe del Banco Mundial sobre perspectivas económicas mundiales (junio 2020), una caída global del 3% y del 5,2% –respectivamente–, asumiendo que si la crisis se supera en la segunda mitad del 2020, en el 2021 la economía crecerá en torno a un 5,8% o 4,2%, según FMI o Banco Mundial. Otro indicador es el referente al desempleo, el cual podría experimentar una pérdida de cerca de 25 millones de empleos. En el campo económico, otro aspecto a tener en cuenta es el cambio de las tendencias en la deslocalización de la producción, avanzando hacia un mayor proteccionismo de los productos nacionales.

“Cambio en la deslocalización de los mercados”

GLOBALIZACIÓN DIGITAL

Es un proceso que podríamos considerar imparable, lo que va a facilitar un profundo cambio en las estructuras de las empresas, avanzando hacia el teletrabajo y disminuyendo sensiblemente los desplazamientos físicos de su personal. Todo ello concede una mayor importancia a las políticas colaborativas.

“Tenemos una capacidad casi infinita para acceder a la información y elegir entre ella, pero eso no nos hace más libres”

Ángel Gómez de Ágreda

INDIVIDUO Y SOCIEDAD

Hasta la expansión de la COVID-19 nuestras sociedades se habían sentido seguras frente a este tipo de amenazas, las cuales se concentraban casi exclusivamente en los países menos desarrollados. Es de prever que una de las consecuencias de esta pandemia será el hecho de

“Tenemos que entender que estamos ante un pasado fallido para gestionar el mundo actual”

que se incremente el sentimiento de miedo a los contagios en los ciudadanos. Lo anterior se podría resumir de manera esquemática tal y como se muestra en la ilustración 4.

ILUSTRACIÓN 4. MANEJAR LA INCERTIDUMBRE



Fuente: Elaboración propia

EL COMPLEJO ESCENARIO ECONÓMICO EN ESPAÑA TRAS LA COVID-19

La pandemia de la COVID-19 ha supuesto un estrés para nuestro sistema sanitario con profundas consecuencias personales y sociales. Además, estamos ante una crisis económica que va a dejar notables secuelas, más agravadas en las clases media y baja de nuestra sociedad.

En particular, se ha estimado que la economía española, una de las más afectadas de los países desarrollados, caerá más de un 12%, afectando a sectores tan importantes como el turismo y los servicios, fundamentales para España, lo que dificultará aún más si cabe la salida de la crisis.

Sin embargo, como en toda crisis, se abren nuevas oportunidades de actividad y negocio, como ya se está poniendo de manifiesto en el ámbito sanitario, farmacéutico, biotecnológico,

telecomunicaciones, inteligencia artificial o ciberseguridad. Esta crisis está impulsando por otra parte el teletrabajo y todo tipo de actividades on line.

Frente a las políticas de la UE, las empresas chinas y anglosajonas son las más beneficiadas, al aprovechar la mayor debilidad de los países europeos, en parte por los elevados índices de deuda pública que tienen la mayoría de sus miembros, siendo España el que posee uno de los más altos, lastrando así su capacidad financiera. Según Hernández de Cos, gobernador del Banco de España, en el escenario de caída del PIB más moderado, la ratio de deuda pública sobre el PIB se elevaría hasta alrededor del 115 %, y en el escenario más adverso se situaría incluso por encima del 120 % del PIB (unos 25 puntos porcentuales más que a finales de 2019).

En este delicado escenario económico, al igual que sucedió en la crisis del 2008, se demuestra la mayor capacidad del sector privado para adoptar medidas eficaces y eficientes, pero, sobre todo, su mayor disposición para adaptarse al cambio, mediante adecuados planes estratégicos que reorienten su actividad con el objetivo de obtener una ventaja competitiva.

Por ello, y ahora más que nunca, **las empresas requieren contar con una superioridad de la información, que lograrán con la adecuada utilización de la inteligencia.** Para enfrentar exitosamente este escenario se precisa desarrollar un modelo de *inteligencia colaborativa* adaptado a las necesidades de las empresas, que les aporta su capacidad de análisis, no solo en el ámbito de la seguridad, sino en el importante campo competitivo, siendo la mejor herramienta para liderar el cambio.

Como botón de muestra del complejo e incierto escenario económico en el que se va a mover España, podemos citar el resumen del FMI, que publicaba *El País*, incluido en la ilustración 5 (*página siguiente*). Se puede apreciar el impacto económico de la COVID-19 con unas caídas de gran calado previstas para 2020, en particular para España, y con unas previsiones para el 2021 ciertamente muy optimistas y a fecha de publicación de esta guía de nuevo modificadas a la baja dada la duración de la pandemia y la desigualdad de gestión de la crisis por los diferentes países, donde España destaca por los pronósticos más intensos.

Así, España, una de las naciones más afectadas, tendrá probablemente una recuperación más lenta de la prevista en la ilustración 5.

Las empresas españolas, ante la debilidad y volatilidad del mercado nacional, se verán obligadas a internacionalizar su actividad, como ya hicieron, por otra parte, en la crisis económica del 2008.

Esta internacionalización requiere hacer un esfuerzo en el ámbito de la inteligencia, esfuerzo que va más allá de la propia seguridad, para entrar en el competitivo, analizando mercados, clientes, o competidores, entre otros, que permitan una toma de decisiones más sustentada.

ILUSTRACIÓN 5. IMPACTO ECONÓMICO DE LA COVID-19



Fuente: El País (mayo 2020)

Los escenarios con mayor nivel de incertidumbre, y en el que nos encontramos sin duda la tiene en grado muy elevado, precisan de una mayor superioridad informativa y ésta solamente la alcanzarán mediante la inteligencia.

EL CONCEPTO DE SEGURIDAD AMPLIADA

Cualquier organización debe garantizar como fin último su supervivencia. Así, la supervivencia del Estado es el bienestar y desarrollo de sus ciudadanos, junto con su integridad territorial y el orden constitucional; si hablamos de la comunidad, su supervivencia es precisamente la identidad de la organización, grupo o etnia; si lo hacemos del medio ambiente, deberemos fijarnos en la sostenibilidad como el pilar fundamental de dicha supervivencia; y si nos referimos a una empresa es precisamente su continuidad de negocio lo que la garantizará finalmente. Podríamos seguir con la enumeración, pero llegaremos a la misma conclusión: ¿cómo garantizar la supervivencia? y la respuesta no es otra que mediante la seguridad.

La seguridad plena es imposible, por ello es necesario plantear tres preguntas fundamentales: ¿qué tenemos que proteger?, nos dirá el objetivo de la seguridad; ¿de qué nos tenemos que proteger?, analiza los riesgos a los que nos enfrentamos; y ¿cómo nos protegemos?, para así determinar los medios y estrategias a aplicar (ilustración 6).

ILUSTRACIÓN 6. LAS TRES PREGUNTAS CLAVE PARA LA SEGURIDAD



Fuente: Elaboración propia

Si bien el fin último de la seguridad (corporativa) sigue siendo la integridad de las personas y la continuidad del negocio, en las últimas décadas el concepto de seguridad ha cambiado de manera notable con respecto a cómo se concebía hace tan solo cincuenta años, entendiéndola en un concepto ampliado.

Como corolario a este cambio en el paradigma de la seguridad, se cambia el concepto de Seguridad Nacional, que abandona la utilización exclusiva de la fuerza y/o la disuasión para enfrentar las amenazas tradicionales, en un modelo en el que se solapaban la seguridad y la defensa nacional, sin que hubiera una diferencia clara entre ellas. Hoy en día esto está superado en la mayoría de las naciones que han desarrollado sus estrategias de seguridad nacio-

nal, entre ellas España, y en las que se reflejan estas tres características citadas para la seguridad de nuestros días: multidimensional, integral y global. En estas estrategias se considera, de hecho, la actividad empresarial como una manera de garantizar y fortalecer los intereses del Estado. Es un nuevo paradigma de seguridad, conocido como Seguridad Ampliada, el que en su momento hemos denominado como seguridad de 360°.

“ ... desde el punto de vista de una seguridad ampliada existen otros objetos referentes, como las personas, las sociedades o el propio planeta. Para los que preconizan esta última visión, y teniendo en consideración el conjunto de nuevas amenazas, la seguridad solo puede ser conseguida equilibrando todos los instrumentos disponibles ... ”

Mario Laborie

Esta visión ampliada de la seguridad se encuentra completamente asumida en el mundo anglosajón, algo de lo que en España todavía estamos lejos, ya que sigue existiendo una brecha entre lo estatal y lo privado, no estando exento de ello la seguridad. Lo primero que se debe entender es que la seguridad no es un asunto asociado de una manera unívoca a lo militar y/o policial, si bien es cierto que hasta mediados del pasado siglo la seguridad (internacional) estaba relacionada casi exclusivamente con las guerras y con la protección del Estado. Finalizada la Segunda Guerra Mundial, y más concretamente con la aparición de la amenaza nuclear, ya no se trataba de cómo ganar una guerra, sino de cómo evitarla, confiriéndole, en consecuencia, una mayor complejidad al problema. Por ello, entre otras razones, los estudios de seguridad pasaron a formar parte de las actividades curriculares de las universidades, incorporándose posteriormente su estudio al ámbito de las ciencias sociales.

Como ya se ha apuntado en el capítulo segundo de esta guía, conviene recordar que los estudios de seguridad se han materializado en las tres visiones clásicas de las relaciones internacionales –realismo, liberalismo y constructivismo–. Las dos primeras ampliamente desarrolladas, sobre todo en Estados Unidos, mientras que al hablar de la tercera es necesario referirnos a Europa, y en particular a la escuela de Copenhague. Europa, y en particular el Reino Unido y Francia, han sabido desarrollar sus propias teorías en las tres visiones ya referidas, contraponiendo frente a Estados Unidos una visión más abierta y ampliada de la seguridad.

A lo anterior habría que añadir, aunque sea brevemente, lo que se conoce como los “enfoques críticos a la seguridad” que con gran acierto desarrollan Shepherd (2013) o Collins (2016). En ellos se incluyen aspectos tan importantes hoy en día como la seguridad humana, la seguridad ambiental o la de género, por citar algunas.

Como todo concepto de amplio espectro, el de la seguridad se enfrenta al eterno problema de su definición. En cualquier libro especializado o buscador en internet encontraremos mu-

chas de ellas, las cuales dependerán en gran medida de quién las origina y en qué momento se definen, lo que posiblemente nos proporcione una percepción un tanto sesgada de ella. En consecuencia, obviando el tema de la definición, vamos a introducir algunas ideas para tratar de comprender mejor este concepto amplio de la seguridad, entendiendo ésta como un estado, una situación, una acción y una función, lo que a su vez nos permitirá visionarla con un enfoque de 360°:

- Como **estado** nos centramos en el objeto a proteger, para reducir su nivel de vulnerabilidad, ya se trate de personas, instalaciones, medios o reputación. En este caso podremos hablar de seguridad humana, del Estado, societal¹, o física, entre otras.
- Atendiendo a la **situación**, nos centramos en las amenazas generadoras de los riesgos a los que nos enfrentamos, los cuales, junto a las vulnerabilidades propias, nos permitirán determinar la probabilidad y el impacto de los riesgos que nos pueden afectar y de esta forma adoptar las medidas preventivas y en su caso reactivas.
- Su visión como **acción** pone el énfasis en lo que se puede y se debe de hacer, es decir, se trata aquí de determinar el proporcionado y adecuado uso de los medios disponibles. En esta parte del análisis de la seguridad es donde se tratan las estrategias de seguridad, las cuales, como toda estrategia, están orientadas a “hacer lo correcto” a diferencia de la táctica, mucho más tangible, que trata de “hacer las cosas bien”.
- Por último, pero no menos importante, desde su dimensión como **función**, se establecen las responsabilidades de los diferentes actores, ya que no sólo se deben involucrar las funciones directivas, pues se orienta a la integración de todos los esfuerzos y en última instancia a la creación de una cultura de seguridad, la cual será una de las principales herramientas para empoderar a la sociedad.

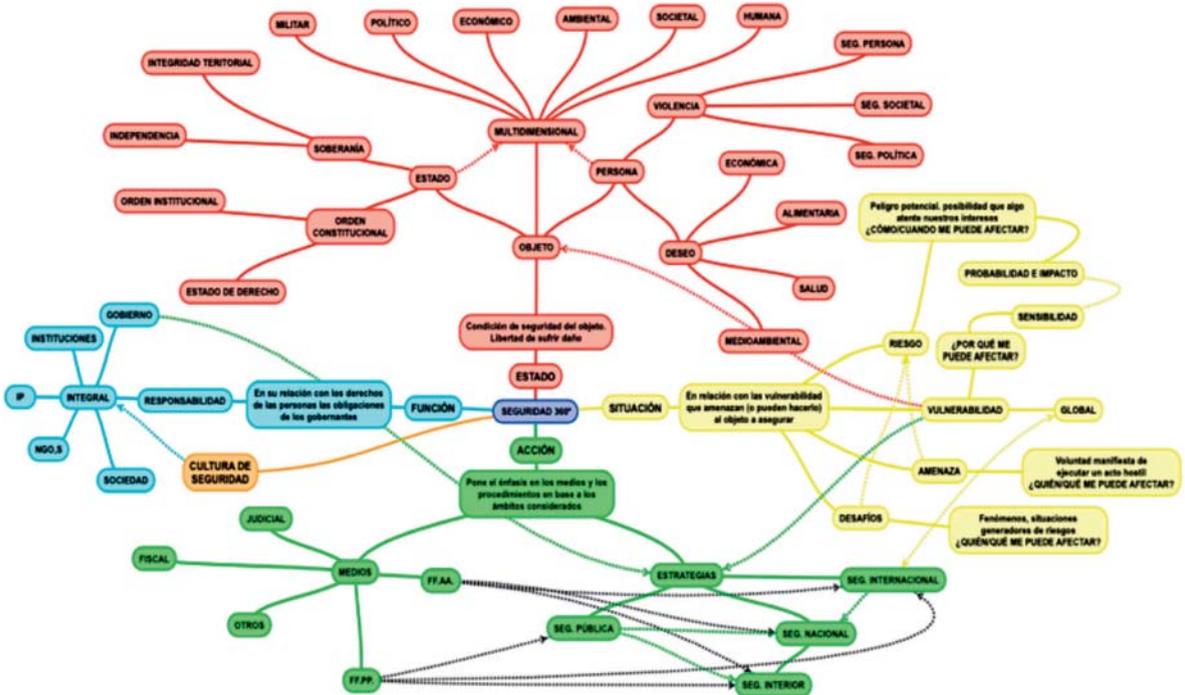
Si llevamos esta conceptualización de la seguridad al mundo empresarial, vemos que, como estado, la seguridad trata de proteger a las personas, las infraestructuras, la marca, la reputación y la continuidad de negocio. Como situación, requiere un exhaustivo y continuo análisis de riesgos y amenazas que le permitan anticiparse a una situación perjudicial para sus intereses, lo que entre otros aspectos aconseja disponer de un adecuado sistema de inteligencia. Como acción, toda empresa deberá tener su plan de seguridad, su plan de continuidad de negocio, así como los necesarios planes de contingencia y tener previsto para cada uno de ellos los medios pertinentes para garantizar su fin último, que es la propia supervivencia de la empresa. Desde la perspectiva de la seguridad como función, debe ser entendida como un proceso transversal que afecta a los diferentes departamentos pero que debe de ser dirigido al más alto nivel de la organización.

1. El término societal es una traducción directa del inglés, refiriéndose a la seguridad de la comunidad, incluyendo sus diferencias culturales, étnicas, religiosas, etc.

Resumiendo, la seguridad desde una visión ampliada debemos verla como: multidimensional, por cuanto abarca diferentes ámbitos de la actividad humana/empresarial; integral, por cuanto requiere la concurrencia de diferentes actores con una sola unidad de esfuerzo, con independencia de la responsabilidad que se asume en su dirección al más alto nivel, y entendida como una de las políticas fundamentales de cualquier Estado o uno de los procesos críticos en una empresa; y global, como consecuencia de la interconexión e interdependencia tecnológica que ha convertido en globales la mayoría de los riesgos a los que se enfrentan nuestras organizaciones y sociedades y por tanto las soluciones deben ser alcanzadas de una manera colaborativa.

En la ilustración 7 incluimos un ejemplo de seguridad de 360° con un diagrama en el que se relacionan los cuatro aspectos mencionados de la seguridad: estado, situación, acción y función. Si bien se refiere al ámbito de la seguridad nacional, es fácilmente extrapolable al de una empresa.

ILUSTRACIÓN 7. LA SEGURIDAD 360°



Fuente: Elaboración propia

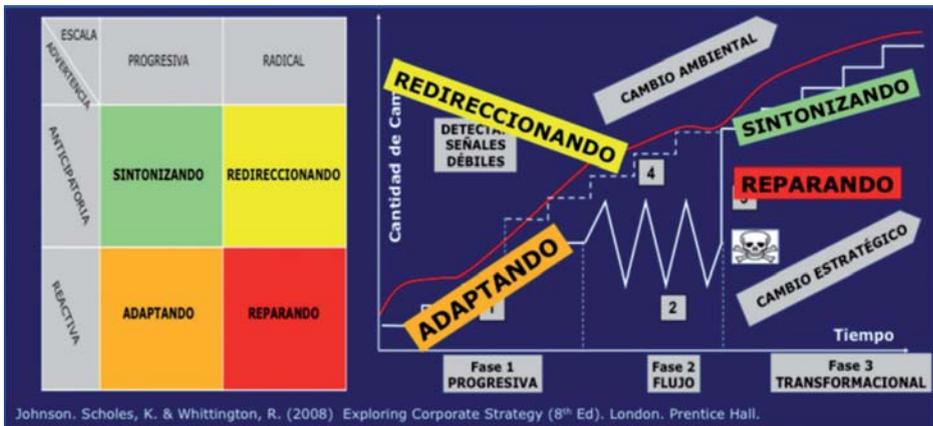
EL MERCADO DE LA INTELIGENCIA. UN MERCADO EN EXPANSIÓN EN LA INTERNACIONALIZACIÓN EMPRESARIAL

La inteligencia es una actividad o función básica en los procesos de toma de decisiones que orientan la actividad y en su caso el cambio de toda organización empresarial. Todo cambio está forzado en ocasiones y siempre condicionado por el contexto en el que se mueve la organización. Quiere decir que además de conocer nuestras propias fortalezas y debilidades, se precisa conocer las oportunidades y amenazas que conforman el contexto en el que desarrollamos nuestra actividad empresarial. La inteligencia es pues la herramienta capital que nos va a facilitar la información precisa sobre los procesos internos, así como del entorno externo, permitiendo con ello alcanzar una posición de ventaja en la toma de decisiones.

A mayor nivel de incertidumbre se manifiestan mayores vulnerabilidades en el ámbito interno, las cuales es preciso detectar y corregir con la mayor precisión y rapidez. Por otra parte, el contexto es mucho más volátil y difuso, por lo que es difícil precisar la curva de ambiente (*en rojo en la ilustración 8*), con el riesgo de que si nos alejamos mucho de ella se corre el riesgo de que la organización se quede obsoleta y comience a tener pérdidas. A su vez, en un ambiente incierto el número de riesgos y amenazas se incrementa notablemente y con ello nuestra vulnerabilidad, lo que debe ser corregido de manera continua.

En la ilustración 8 se expone un gráfico de la curva de Scholes con las variables de Naddler que se muestran a la izquierda de la imagen para una mejor comprensión de la complejidad del cambio y la importancia que tiene para las empresas contar con la función de inteligencia.

ILUSTRACIÓN 8. LA INTELIGENCIA EN LOS PROCESOS DE CAMBIO



Fuente: Elaboración propia con datos de Exploring Corporate Strategy. Scholes y Naddler (última ed.)

Por todo ello, si ya hemos establecido la importancia de la inteligencia en la toma de decisiones, cuando –como en el caso del actual escenario geoestratégico mundial– nos encontramos en una situación de gran incertidumbre, la inteligencia cobra una importancia capital para cualquier organización. Las empresas, como organizaciones cuya actividad se desarrolla en un escenario complejo e incierto precisan contar con una superioridad de la información, a la cual se llega precisamente mediante la inteligencia.

Es por lo anteriormente expuesto por lo que podemos considerar que la inteligencia es un mercado en alza, porque las empresas necesitan de esta función más que nunca. La parte positiva a esta necesidad es que hoy en día esta función se ve facilitada por el desarrollo de las nuevas tecnologías. Éstas facilitan la interconexión y la cooperación, lo que da sustento al concepto de inteligencia colaborativa, la cual permite alcanzar grandes objetivos con unos medios reducidos y un gasto asumible por la mayoría de las organizaciones empresariales.

“La inteligencia es una necesidad para cualquier pyme en sus procesos de internacionalización en un entorno cada vez más complejo e incierto. Por ello, la inteligencia puede considerarse como un mercado en alza”

A continuación, se destacan algunos de los criterios por los que se puede considerar a la inteligencia como un mercado en expansión: rentabilidad económica, seguridad de viajeros, producto externo (*outsourcing*), a mayor incertidumbre mayor necesidad de inteligencia, apoyar el mercado nacional en el sector de la inteligencia y la seguridad, un

producto específico para cada empresa, orientar el producto de inteligencia a las pymes y los valores de una compañía de inteligencia colaborativa.

RENTABILIDAD ECONÓMICA

Las empresas españolas exportaron por valor de 267.500 M€ en 2019 y deberán continuar esta tendencia alcista para subsistir, debido a la ralentización del mercado nacional y al impacto económico de la crisis vírica.

El escenario económico que se presenta tras la COVID-19, ya expuesto brevemente en el capítulo 3, obliga por una parte a conferir una mayor importancia a la inteligencia económica, al objeto de rentabilizar nuestro negocio. Por otra parte, si tenemos en cuenta la situación económica en el interior del país, será necesario continuar con el impulso de los procesos de internacionalización, lo que pone claramente en valor tanto la inteligencia competitiva como la relacionada con la seguridad física.

SEGURIDAD DE VIAJEROS

Si los procesos de internacionalización aumentan lo harán también los desplazamientos de personal al exterior, tanto los que se desplacen de una manera semipermanente, como los que realicen viajes de supervisión y/o implantación del negocio.

Necesitan por ello de manera fundamental los productos de inteligencia y seguridad de los viajeros en sus desplazamientos internacionales, entre los que se incluyen un adecuado sistema de alertas, de atención sanitaria, de geolocalización y, llegado el caso, de apoyo en la evacuación. El deber de cuidado se impone como factor de retención y obligación legal.

PRODUCTO EXTERNO (*OUTSOURCING*)

Muchas de las grandes empresas, conscientes de la importancia de la inteligencia, han incluido en su estructura organizacional un departamento y/o función de inteligencia. Otras, aunque aún hoy en día en porcentaje muy pequeño, contratan este tipo de productos y/o servicios a empresas especializadas del sector.

Como ya se ha mencionado en estas páginas, a mayor complejidad e incertidumbre del entorno, mayor es la necesidad de contar con los servicios de inteligencia. Es por ello por lo que en el contexto actual se podría considerar casi como una exigencia contar con este tipo de servicios tanto para las grandes como las medianas y pequeñas empresas.

A MAYOR INCERTIDUMBRE MÁS INTELIGENCIA

Por las razones ya expuestas, la previsión es que el mercado de la inteligencia tendrá crecimientos exponenciales en el próximo quinquenio.

Hoy en día, salvo en el mundo sajón, existe un número reducido de empresas especializadas en inteligencia colaborativa, siendo una solución de valor añadido para las medianas empresas, considerando que las grandes tienden a tener sus propios recursos de inteligencia. Pero aún en este caso, su dimensión no les permite absorber la totalidad de los asuntos, por lo que para ellas también es necesario contar con servicios externos.

APOYAR E IMPULSAR EL MERCADO NACIONAL EN EL SECTOR DE LA INTELIGENCIA Y LA SEGURIDAD

Los suministradores actuales de productos de inteligencia son mayoritariamente anglosajones, lo que en muchas ocasiones es puesto en duda por el mercado interno.

Para construir un mercado propio es necesaria la acción concertada de ambas partes: las empresas como clientes y receptores del producto y las compañías suministradoras de los servicios de inteligencia y seguridad. Ésta debe ser una actividad concurrente para poder consolidar a nuestras compañías en los niveles más altos del mercado.

PRODUCTO ESPECÍFICO PARA CADA EMPRESA

Existe una percepción hacia estas compañías como demasiado genéricas, en parte porque, como se ha dicho en el apartado anterior, son compañías con dificultades para conocer la integridad del mercado y empresariado español al atender de una manera global a un gran número de clientes, teniendo además unos mayores costes y aportando por tanto poco valor añadido como consecuencia de su carácter generalista.

CÓMO ORIENTAR EL PRODUCTO DE INTELIGENCIA PARA EL USO POR LAS PYMES

Las grandes empresas de seguridad privada españolas han comenzado a tener estos productos en su catálogo, conocedoras de la demanda actual. Se trataría ahora de ponerlos en valor en las pymes, como ya se ha citado anteriormente, con unas condiciones de coste accesible, alta rentabilidad, valor añadido y personalización conforme a sus necesidades

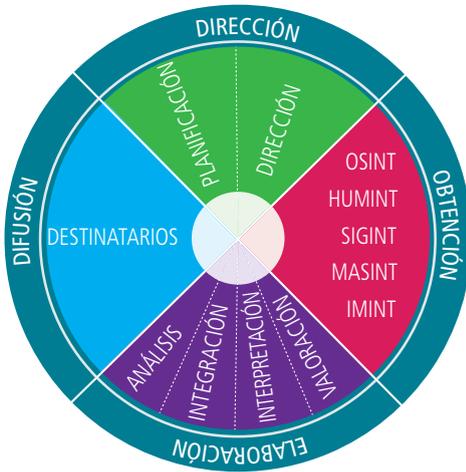
VALORES DE UNA COMPAÑÍA DE INTELIGENCIA COLABORATIVA

Los factores críticos para el éxito son: la **especialización**, que requiere de profesionales competentes con amplios conocimientos y experiencia; la **ética**, ofreciendo productos de calidad y obteniendo la información de manera legal y legítima; la **confianza**, basada en los productos ofrecidos; y la **fiabilidad** de los resultados y personalización, evitando productos generalizados y proporcionando un servicio adaptado a las necesidades de cada pyme.

LA APLICACIÓN DE LA INTELIGENCIA PARA LA SEGURIDAD EN LAS PYMES ¿ES TU NEGOCIO SEGURO?

La inteligencia genera conocimiento (especializado) y es el resultado de un proceso sistemático y normalizado que transforma la información disponible y/u obtenida por medios y recursos dispares, incluso con métodos diferentes, basados en fuentes abiertas (OSINT) como en las humanas (HUMINT) u otras.

ILUSTRACIÓN 9. EL CICLO CLÁSICO DE INTELIGENCIA



Fuente: Elaboración propia

ILUSTRACIÓN 10. LA INTELIGENCIA CENTRADA EN EL OBJETIVO



Fuente: Elaboración propia

El tradicional CICLO DE INTELIGENCIA se compone de varias fases (Ilustración 9): la **dirección**, mediante la que se planifica el proceso, determinando las necesidades y objetivos; la **obtención**, en la que se obtiene la información de diferentes fuentes, abiertas (OSINT), humanas (HUMINT), señales (SIGINT), imágenes (IMINT) y actualmente unas que han cobrado una importancia relevante como son las de las redes sociales (SOCMINT); la **elaboración** es la parte medular del proceso, pues es lo que permite la transformación de la información en inteligencia, y dentro de ella es el análisis el nudo gordiano del sistema, no en vano es el producto de inteligencia que va a llegar al tomador de decisiones; por último, la fase de **difusión** es la que lleva la inteligencia al consumidor, bajo un principio fundamental cual es el de "necesidad de conocer" que quiere decir que la inteligencia debe llegar al que debe explotarla y solamente aquella parte que realmente le interesa.

Hoy en día este ciclo ha cambiado ligeramente hacia el concepto de la **inteligencia centrada en el objetivo** (Ilustración 10). La caracterís-

tica de este nuevo concepto del ciclo de inteligencia es que en él se integran todas las partes interesadas o grupos de interés (*stakeholders*), incluidos los usuarios directos (clientes) y otras agencias y/o servicios. El motivo es que el objetivo ya no es un elemento simple, sino que es extraordinariamente complejo en el que quedan integrados diferentes actores y procesos todos ellos relacionados e interactuando entre sí, de manera que se precisan diferentes elementos que colaboren para obtener una información completa que permita construir una inteligencia lo más precisa posible. De una manera esquemática lo podríamos representar como se muestra en la ilustración 11. Esta es, como veremos más adelante, una de las razones por las que la **inteligencia colaborativa es un valor en alza**.

Es un nuevo concepto que se conoce como producción basada en el objetivo (OBP, por sus siglas en inglés), que supone organizar el esfuerzo de inteligencia en los objetos de interés. Como nos indica Clark (2017), *con ello se presenta un intercambio del estado de conocimiento del objetivo de inteligencia "basado en la nube" (Intelligence Analysis)*. En este intercambio se incluyen las diferentes partes interesadas.

Como se aprecia en la ilustración 11 es un proceso continuo sobre el objetivo en el que participan todos los *stakeholders*.

ILUSTRACIÓN 11. EL CICLO DE INTELIGENCIA BASADO EN EL OBJETIVO



Fuente: Elaboración propia

"Cada uno de los pasos del ciclo de inteligencia se está produciendo continuamente y sobre cualquier asunto"

Robert M. Clark

Al referirnos a la inteligencia relativa a las empresas se podría caer en la tentación de simplificar el concepto para reducirlo al espionaje (industrial), el cual no es sino un medio de obtención del que no se hace mención en esta guía, por cuanto es una práctica en el mundo empresarial no aceptada habitualmente desde una perspectiva tanto de la ética, como con base en su legitimidad. Pero sí es bueno tenerlo en cuenta en la medida que una de las funciones que cubre la inteligencia es precisamente la protección de la información propia —contrainteligencia—, para lo cual se supone que se deben establecer los procedimientos para evitar cualquier tipo de intrusión, entre ellos el espionaje (industrial).

Las necesidades de inteligencia de las empresas se podrían agrupar en dos grandes bloques, la inteligencia competitiva y la inteligencia para la seguridad, ambas serán desarrolladas de una manera más amplia en los dos siguientes apartados.

En ambos casos, se podría afirmar sin temor a equivocarnos que el análisis es vital en la producción de inteligencia:

- El análisis puede tomar muchas formas y recurrir a muchas fuentes, es frecuente utilizar varias de ellas para tener una imagen lo más amplia del problema, lo cual abunda en la importancia de la inteligencia colaborativa.
- Se trata de un proceso continuo. Las empresas (pymes) precisan del apoyo constante (diario) en materia de inteligencia, ya sea por medio de un sistema de alertas generales, como específicas para cada una de ellas.

¿Por qué es importante la inteligencia para las empresas? En la ilustración 12 se puede apreciar un resumen que responde a la pregunta.

ILUSTRACIÓN 12. ¿POR QUÉ ES IMPORTANTE LA INTELIGENCIA PARA LAS EMPRESAS?

La inteligencia es una actividad crítica para la seguridad y la competitividad de cualquier organización

- 1 INCERTIDUMBRES A NIVEL MUNDIAL
- 2 GLOBALIZACIÓN DE LOS MERCADOS
- 3 REPUTACIÓN DE LA EMPRESA
- 4 ANTICIPARSE Y MITIGAR SITUACIONES DE CRISIS
- 5 ASEGURAR RESILIENCIA ORGANIZACIÓN
- 6 PROTEGER ACTIVOS FRENTE A RIESGOS Y AMENAZAS
- 7 OBTENER VENTAJAS COMPETITIVAS

“Todos los usuarios-demandantes de servicios de inteligencia exigen cada vez más detalles sobre los objetivos”

Robert M. Clark

LA INTELIGENCIA COMO HERRAMIENTA PROACTIVA

No se trata simplemente de reaccionar ante situaciones no deseadas o de la búsqueda de soluciones ante un problema concreto –inteligencia reactiva–, sino de estar en condiciones de anticipar situaciones que, sin ser necesariamente originadas por un acontecimiento dramático, como es el caso de la COVID-19, aconsejan anticipar medidas para lograr o mantener la ventaja competitiva y la continuidad de negocio –inteligencia proactiva–.

La inteligencia es en sí misma proactiva y reconoce que la ausencia de acontecimientos dramáticos no asegura una ausencia de amenazas competitivas, estando orientada, en consecuencia, a la detección de señales de alerta y a la prevención de riesgos.

Cada cambio en el entorno origina señales y mensajes que las organizaciones deben conocer e interpretar. Estas señales se producen tanto en el entorno inmediato –proveedores, competidores, socios, clientes– como en el contexto general en el que se incluyen los factores económicos, tecnológicos, políticos o sociales.

Uno de los beneficios del análisis de señales de alerta es su contribución a la gestión del riesgo estratégico, entendiéndose por tal la existencia de un acontecimiento inesperado o un conjunto de condiciones que reducen significativamente la habilidad y la posibilidad de los directivos para implementar con éxito su estrategia de negocio.

Si aceptamos que lo que crea el riesgo es la incertidumbre y lo que crea incertidumbre tiene que ver con el cambio, debemos considerar que, para hacer frente al riesgo, uno de los primeros pasos es identificar los factores de cambio (tecnológicos, nuevas regulaciones, acciones políticas y/o gubernamentales, o tendencias sociales, entre otros) de un sector o una industria.

Frente a la gran diversidad de variables que se precisan controlar y que pueden tener un impacto en el desarrollo del negocio, cada vez es más patente la necesidad de aplicar medidas de inteligencia proactiva.

La inteligencia, bajo una dirección única, se desarrolla en tres niveles: estratégico, operacional y táctico, los cuales aplicados a la empresa se podrían entender tal y como se expone a continuación.

- El NIVEL ESTRATÉGICO corresponde, refiriéndonos al mundo empresarial, casi con exclusividad a la inteligencia competitiva, se encuentra íntimamente vinculado con el análisis estratégico para detectar y orientar los indicadores del cambio y comprende una combi-

nación de recursos, capacidades y estrategias para tener una ventaja competitiva, tanto en lo que se refiere al desarrollo del porfolio adecuado, la configuración de los procesos, dónde vamos a desarrollar con mayor éxito nuestra actividad y la identificación de los factores de éxito.

- El NIVEL OPERACIONAL, lo podríamos aplicar en el lanzamiento y comercialización de un determinado proyecto o servicio. Por ejemplo, si una empresa de energías renovables tiene intención de abrir un parque eólico, se precisa un complejo proceso de inteligencia para conocer en detalle su impacto, o los intereses y previsibles reacciones de todos los grupos de interés. En este nivel se produce un equilibrio entre los intereses competitivos y los de seguridad.
- Por último, el NIVEL TÁCTICO es el que pretende tener el conocimiento más amplio del desarrollo de negocio y la seguridad del personal y los activos de la empresa. En este nivel la seguridad es fundamental, por cuanto está íntimamente relacionada con la continuidad del negocio y resulta prioritaria la detección oportuna de cualquier riesgo o amenaza que pueda comprometerlo. En este sentido, en el marco de la inteligencia competitiva será preciso tener presente en todo momento la cadena de valor de la empresa, mientras que la inteligencia de seguridad, basada en un adecuado sistema de alertas, se orientará a la protección de sus activos.

La tabla 3 nos daría una aproximación al nivel de seguridad que tiene nuestro negocio, nuestra empresa, organización y/o pyme, después de analizar los ámbitos marcados en afirmativo y en negativo.

TABLA 3. NIVEL DE SEGURIDAD

#	ASUNTO	SI	NO
1	Conoce adecuadamente los riesgos y amenazas a los que se enfrenta su organización	●	●
2	Tiene adecuadamente protegidos su información y procesos	●	●
3	Realiza auditorías de seguridad con una periodicidad al menos anual	●	●
4	Tiene su empresa un responsable de seguridad	●	●
5	Su personal está geolocalizado en sus desplazamientos	●	●
6	Dispone de un sistema de alarmas que le permita anticipar una situación no deseada	●	●
7	Dispone de un plan de seguridad en su empresa y en las diferentes instalaciones de esta	●	●
8	Cuenta con un servicio de inteligencia que le prevenga de los posibles riesgos y amenazas	●	●

Fuente: Elaboración propia

Las preguntas planteadas en la tabla 3 no constituyen una lista cerrada, se pueden incluir otros ítems que abunden en el mejor conocimiento del grado de seguridad que tiene la empresa. En esta lista de verificación o *check list* se utiliza el método semáforo, de manera que lo que aparezca en color rojo deberá ser objeto de modificación pues representa una debilidad.

Un aspecto fundamental a la hora de determinar el grado de seguridad que tiene nuestra organización es un conocimiento lo más amplio posible de su entorno, ello pasa en primer lugar por tener identificados y valorados los riesgos y las amenazas a los que se enfrenta (ítem 1).

El resto de las cuestiones tienen que ver con el contexto interno de la organización, lo que finalmente determinará sus fortalezas y debilidades, debiendo corregir estas últimas para disminuir las vulnerabilidades de la empresa. Los ítems 2, 5, 6 y 8 tienen que ver con medidas de protección, en consecuencia, una respuesta negativa supone un mayor grado de vulnerabilidad y como resultado que el impacto de una emergencia o situación desfavorable sea mayor. Es importante llamar la atención sobre la conveniencia de contar con un plan de seguridad acorde con la entidad y actividad de la empresa (ítem 7). Esto último estaría relacionado con la conveniencia de disponer de un jefe de seguridad (ítem 4), si bien esto es algo que en muchas ocasiones queda fuera del alcance de una pyme, pero que puede ser realizado por una organización externa (prestación de un servicio) a través de una empresa especializada de las que cada vez más, como hemos indicado, existen en el mercado nacional.

Por último y no menos importante es lo que se refiere a las auditorías de seguridad (ítem 3), algo que toda organización debe realizar periódicamente pues ayuda a identificar las desviaciones sobre los planes iniciales y el grado de cumplimiento de los procedimientos de los diferentes procesos que tienen que ver con la seguridad. Aunque las auditorías pueden ser internas o externas, son más recomendables estas últimas, pues en las primeras hay una tendencia natural a enmascarar las debilidades de la organización.

LA INTELIGENCIA COMPETITIVA ¿ES TU NEGOCIO COMPETITIVO?

En el apartado anterior hemos determinado el grado o nivel de seguridad que tiene la empresa en cuestión, en este epígrafe —y teniendo en cuenta todo lo que ya se mencionó sobre el concepto y evolución de la denominada IC— vamos a tratar de la protección de su competitividad.

La competitividad de una organización es fundamental a la hora de realizar el análisis estratégico que nos determine los objetivos a alcanzar, así como identificar nuestros principales competidores y colaboradores.

De acuerdo con Zanoni (2012) es necesario comprender cuál es la estructura competitiva, es decir los principales elementos que la componen:

- La combinación de recursos, capacidades y competencias estratégicas.
- La cartera de tecnología de la producción.
- La posición competitiva.
- La configuración de los procesos.
- Los ámbitos competitivos.
- Los factores críticos de éxito, las fortalezas y las eventuales debilidades.
- Las posiciones competitivas resultantes.

“En un escenario global en el que todo, desde las finanzas hasta la cadena de suministro, está tan altamente integrado, las barreras a la competencia que una vez protegieron a las empresas, sectores y territorios se están volviendo cada vez menos restrictivas y resistentes”

Andrea Beretta Zanoni

Ya hemos visto en los puntos anteriores que el planeamiento debe estar fundamentado en la información y ésta será de poco o nulo valor si no está contextualizada y analizada convenientemente, es decir transformada en inteligencia. Como nos dicen Ortoll y García (2015), ésta es resultado en primer lugar, de la captura de información tanto interna como externa a la organización y, en segundo lugar, del análisis, interpretación y valoración

de esta información. Entendido así es un producto y un proceso, orientado al diseño estratégico de la empresa y a la toma de decisiones.

A veces se utilizan términos como el de *inteligencia económica*, orientada a la mejora económica de las empresas, o, también, el de *inteligencia de marketing*, centrada en la información del mercado. Sin embargo, la IC analiza e interpreta temas de negocio más amplios y

polifacéticos, va más allá del mero estudio de mercado, para atender otros aspectos del entorno de la organización (tecnológicos, sociales o políticos).

Las mismas fases que hemos visto en el punto anterior son válidas al hablar de la IC, siendo de particular importancia, además de lo mencionado para el análisis, la determinación de las necesidades, que corresponde a la alta dirección. En este sentido cabe mencionar la marcada influencia que sobre ella ejerce la cultura organizativa de la empresa, siendo importante señalar que las corporaciones que conceden una mayor importancia a la inteligencia como sistema para crear valor, tienen más fácil alcanzar la deseada ventaja competitiva.

En la citada publicación *La Inteligencia Competitiva* (Ortoll y García, 2015) —así como en la bibliografía citada en el capítulo segundo de esta guía— se hace hincapié en que la función de inteligencia tiene que estar alineada con los objetivos operativos y estratégicos de la organización, identificándose seis ámbitos de aplicación:

- **Inteligencia de negocio**, orientada a los procesos de negocio con información proveniente de los sistemas internos (existencias, suministros, recursos humanos, clientes, etc.).
- **Inteligencia del competidor**, conducente a obtener información sobre los competidores actuales y potenciales.
- **Inteligencia de mercado**, identifica las tendencias actuales y futuras de las necesidades y preferencias de los clientes, nuevos mercados o la propia percepción de la empresa.
- **Inteligencia comercial**, dirigida al proceso de producción y a la obtención de información sobre nuevos productos y tecnologías.
- **Inteligencia tecnológica**, para detectar las oportunidades y amenazas que generan las nuevas tecnologías y determinar su impacto en el negocio.
- **Inteligencia del entorno**, observa el conjunto de los aspectos político-sociales, culturales, legales, medioambientales que configuran el escenario en el que actúa la empresa.

También cabe aquí la diferenciación entre la IC en el nivel estratégico, cuyo objetivo es detectar señales de alerta, oportunidades y amenazas para apoyar las decisiones en el largo plazo. Si nos referimos al nivel táctico, la IC sirve de apoyo a los procesos operativos de la organización, a la actividad diaria. Entre ambas está el nivel operacional, cuando se centra en un proyecto en concreto, por ejemplo, cuando una empresa en su programa de internacionalización busca oportunidades de negocio en diferentes lugares.

Existen diversos métodos para el estudio de los factores que nos apoyan para desarrollar un producto de IC. Entre ellos procede destacar el PESTLE (políticos, económicos, sociales, tecnológicos, legales y medioambientales, por sus siglas en inglés) como herramienta de análisis del entorno, basado fundamentalmente en fuentes abiertas; y el DAFO (debilidades, amenazas, fortalezas y oportunidades), válido para el análisis externo (oportunidades y amenazas) y el interno (fortalezas y debilidades). Una herramienta que resulta fundamental en los procesos de inteligencia competitiva para entender el negocio es la cadena de valor, la cual per-

mite un análisis interno de las empresas para entender sus actividades, las relaciones entre ellas y el valor que cada una aporta (Ilustración 13).

ILUSTRACIÓN 13. LA CADENA DE VALOR



Fuente: www.cadenadevalor.com

Finalmente, el diamante de Porter (2004) nos permite analizar la capacidad de innovación de la organización, especialmente indicado cuando una organización decide adoptar un cambio (Ilustración 14). Esta herramienta permite identificar las barreras que se oponen a él.

ILUSTRACIÓN 14. EL DIAMANTE DE PORTER



Fuente: Elaboración propia a partir de Porter (2004)

“En el campo de la inteligencia competitiva las compañías especializadas ofrecen a las pymes alertas estratégicas e informes ejecutivos”

Portfolio TWCI

En este sentido, y en función de la utilidad de esta guía, podríamos preguntarnos ¿una pyme, organización, empresa, qué servicios podría recibir/demandar desde un proveedor externo o empresa de servicios de seguridad e inteligencia estratégica? En nuestra opinión estos serían las

alertas estratégicas y los informes ejecutivos. Las primeras son unos indicadores de situaciones tanto de ambiente, externas, como en relación con los procesos, internas. Estas alertas permiten identificar, valorar y analizar las tendencias que permitirán construir escenarios. Por otra parte, esta herramienta permite detectar de manera oportuna los posibles riesgos y de esta forma adoptar medidas proactivas que protejan nuestra organización y garanticen la continuidad de negocio.

Incluimos a continuación, como ejemplo (Ilustración 15), un tipo de alerta de las que se manejan en los procedimientos de TWCI.

ILUSTRACIÓN 15. TIPO DE ALERTA

BOTSWANA publicado el 18.04.2020

1. Pasajeros que llegan de Austria, Bélgica, China (República Popular), Dinamarca, Francia, Alemania, India, Irán, Italia, Japón, Corea (República), Países Bajos, Noruega, España, Suecia, Suiza, Estados Unidos o Reino Unido no pueden ingresar a Botswana.
Esto no aplica a los nacionales y residentes de Botswana.
2. Los nacionales y residentes de Botswana serán puestos en cuarentena durante 14 días.
3. Los pasajeros ya no pueden obtener una visa a su llegada a Botswana.
4. Visas emitidas a ciudadanos de Austria, Bélgica, China (República Popular), Dinamarca, Francia, Alemania, India, Irán, Italia, Japón, Corea (Representante), Países Bajos, Noruega, España, Suecia, Suiza, EE.UU. Están invalidados.
5. Las visas emitidas a pasajeros con pasaporte británico con nacionalidad “Ciudadano Británico” son inválidas.

Fuente: TWCI

Los informes ejecutivos no se limitan a una exposición de datos, sino que debidamente organizados y analizados permitirán generar el conocimiento necesario que abunde en la continuidad del negocio, en obtener una ventaja competitiva e introducir los cambios que se estimen necesarios en la organización. Estos informes pueden ser los que se denominan informes riesgo-país, en los que sobre la base del PESTLE se realiza un análisis del ambiente, indicando los principales riesgos que pueden afectar a la producción/actividad, así como a

las condiciones del país o zona que favorecen o dificultan el desarrollo del negocio. Además de estos informes ejecutivos que suelen ser algo genéricos, existe la opción de elaborar informes corporativos en los que se da respuesta a las necesidades manifestadas por las respectivas empresas (usuarios-demandantes). En la ilustración 16 se puede ver un esquema de los elementos que pueden componer un informe ejecutivo.

ILUSTRACIÓN 16. ESQUEMA DE INFORME EJECUTIVO



Fuente: Elaboración propia

Los cambios organizativos son una de las tareas más complejas a las que se enfrenta una organización, máxime si el cambio viene motivado por un agente externo, como podría ser la situación de algunas pymes tras la COVID-19. Para el diseño estratégico es capital la concurrencia de la inteligencia competitiva, especialmente si se trata de cambios estructurales.

Como ya hemos indicado a lo largo de esta guía, también es importante contar con una adecuada inteligencia competitiva, cuando se trata de los **procesos de internacionalización**, por cuanto aporta un conocimiento amplio de las zonas en las que se va a iniciar la actividad

productiva y/o comercial. Es lo que se podría denominar como **inteligencia territorial**, de hecho, uno de los principales problemas en los procesos de internacionalización es no conocer el territorio en el que se pretende desarrollar la actividad, lo cual no se refiere solamente al entorno, sino a la regulación existente en los diferentes sectores de la economía del país, el nivel de desarrollo tecnológico y la capacidad formativa de los habitantes.

En síntesis, la inteligencia competitiva tiene que ver con la gestión del conocimiento en toda la estructura empresarial, lo que supone un verdadero valor añadido.

Como en el apartado anterior, se incluye una lista de verificación- *Check list* al objeto de evaluar hasta qué punto su empresa es competitiva (tabla 4).

TABLA 4. NIVEL DE COMPETITIVIDAD

#	ASUNTO	SI	NO
1	Tiene definidos los procesos de producción	●	●
2	Dispone de un servicio de inteligencia competitiva	●	●
3	Cuando se toma la decisión de abrir la actividad en un mercado exterior se solicita algún informe de inteligencia	●	●
4	Dispone de un sistema de alertas	●	●
5	Tiene desarrollada su cadena de valor	●	●
6	Conoce la competencia en los nuevos mercados	●	●
7	Mantiene relación con autoridades locales en los diferentes niveles de gobierno	●	●
8	¿Con qué frecuencia realiza auditorías (externas)?	●	●

Fuente: Elaboración propia

Como en el caso de la seguridad de la organización, debemos evaluar los aspectos relacionados con la competitividad de la empresa, pues no olvidemos que uno de los objetivos principales de la inteligencia competitiva es facilitar que la organización/empresa obtenga una posición de ventaja competitiva.

Algunos de los ítems (3, 4 y 7) incluidos en la tabla 4 tienen que ver con el contexto externo de la organización, como es el caso de contar con un informe detallado de inteligencia económica y competitiva antes de abrir nuevos mercados y/o productos; se precisa tener activado un sistema de alertas tempranas que nos permita anticiparnos a situaciones no deseadas y que, por otra parte, nos facilite lograr la ventaja competitiva; también es necesario establecer una red de contactos y relaciones con diferentes autoridades en los distintos niveles de la administración (nacional, regional y local), no se debe olvidar que en determinados casos estos pueden actuar como apoyo relevante.

Otros están vinculados al ámbito interno (ítems 1, 2, 5, 6). El primero es algo fundamental para cualquier empresa como son los procesos de producción como elemento fundamental a proteger; en el ítem 2 se aboga por disponer de un departamento de inteligencia competitiva, sin embargo, es algo que pocas empresas pueden asumir, especialmente pymes, recurriendo a la externalización de este servicio por compañías especializadas; otro aspecto esencial a evaluar desde el punto de vista de la inteligencia competitiva es la cadena de valor por cuanto nos ayudará a identificar los aspectos fundamentales de la producción y la sensibilidad que cada uno de los procesos y activos tienen en la empresa; el cuarto de los aspectos relacionados tiene que ver con los competidores, siendo éstos uno de los *stakeholders* que en mayor profundidad debemos conocer.

Como en el caso de la inteligencia para la seguridad, en un esquema de inteligencia competitiva es fundamental contar con un servicio de auditoría para detectar de manera temprana las vulnerabilidades que tiene la empresa desde una perspectiva competitiva.

EL MODELO DE INTELIGENCIA COLABORATIVA EN EL NUEVO ENTORNO ESTRATÉGICO MUNDIAL

En ciertos ámbitos se entiende que el término **inteligencia colaborativa** significa elegir la mejor opción para alcanzar una determinada meta trabajando en conjunto.

Esta interpretación es una aproximación basada en la etimología de las dos palabras que la componen, inteligencia y colaborar, pero que nos sirve como base para entender una descripción más completa.

Se trata de una forma de **inteligencia emergente** que resulta de la interacción de muchos individuos que se interrelacionan entre sí en el contexto de la cultura digital, pudiendo ser definida como:

“La inteligencia colaborativa supone una deliberación ordenada, facilitada por tecnologías sociales, que permite a un conjunto de personas crear un mejor conocimiento compartido y tomar decisiones, con mayores posibilidades de superar los retos y dificultades que plantean las distintas actividades humanas en un entorno cada vez más complejo y cambiante.” (ICXCI, Innovation Center for Collaborative Intelligence).

En esta definición se incluyen las que son las principales señas de identidad de la inteligencia colaborativa. La primera de ellas se refiere a la necesidad de compartir el conocimiento; cuanto más compartamos más tendremos. El mercado requiere respuestas rápidas y con experiencia y para ello se precisa compartir conocimientos. Es necesario saber cómo y a quien preguntar los tipos de preguntas que abren nuestras mentes a nuevas posibilidades. En una palabra: colaborar.

Si nos ceñimos al ámbito de compartir el conocimiento, se limitaría al concepto de inteligencia colectiva en la que mediante la concurrencia de las acciones de un grupo de personas se llegaría a un producto final. Sin embargo, la segunda de las señas de identidad de la inteligencia colaborativa es que se mueve en el entorno de las tecnologías sociales, según la definición de ICXCI.

En las empresas, hoy más que nunca que vivimos en un mundo global y digital donde las tecnologías de la información avanzan a pasos agigantados, empieza a ser necesario potenciar la **inteligencia colaborativa para conseguir compañías inteligentes**, capaces de adaptarse a cualquier cambio y necesidad.

La tercera de las señas de identidad propuestas en la definición se refiere al entorno, como todo producto de inteligencia, también en este caso se encuentra orientado a la toma de decisiones, poniendo el énfasis en que se producen, hoy más que nunca, en un entorno complejo y cambiante

Para ser competitivo en nuestra economía global, debemos aprender a pensar de manera colaborativa e innovadora. Son muchas las organizaciones que desde hace unos años apuestan por el reclutamiento y la retención de talento corporativo, con lo que partimos de la base de que contamos con empresas repletas de talento y de ideas innovadoras que encuentran un terreno propicio en los entornos que favorecen la colaboración, y que por supuesto cuentan con los recursos tecnológicos y la financiación para poder llevar a cabo proyectos ambiciosos.

"The fact that we are different doesn't mean that one of us is wrong. It just means that there's a different kind of right"

Faith Jegede

Ya hablábamos en el apartado 6 de la complejidad del objetivo de la inteligencia, que quiere decir que se debe buscar la colaboración entre diferentes elementos para generar el conocimiento necesario en un mundo interconectado como el actual; por ello se precisan equipos más

perspicaces, más rápidos e innovadores que nunca. La inteligencia colaborativa requiere que abandonemos las formas cómodas y habituales de pensar con los demás y abramos la mente para poder reconfigurar nuestro enfoque.

La inteligencia colaborativa también puede clasificarse de acuerdo con el grado y tipo de colaboración que los individuos aporten al producto final, pudiendo producirse de las siguientes maneras, que a su vez están definidas en Wikipedia como resultante de inteligencia colaborativa en un modo fusión:

- **Modo fusión**, donde cada individuo aporta al producto final, donde esta contribución queda fusionada. Este es el caso de los artículos de la Wikipedia.
- **Modo molecular**, como es el caso de un libro escrito por varios autores, donde cada contribución conserva su identidad relativa dentro de la entidad mayor.
- **Modo colección**, donde las contribuciones aportan a un conjunto mayor que puede resultar abierto.
- **Modo agregación**, como es el caso de las contribuciones a los *blogs* o los artículos en los medios de comunicación.

En el caso de las compañías proveedoras de servicios de inteligencia colaborativa, combinan todos los tipos de colaboraciones: de fusión, generando así un mayor nivel de conocimiento procedente de fuentes especializadas; molecular, recurriendo a la suma de capacidades de diferentes actores, integradas en una entidad única; y los modos de colección y de agregación, mediante la configuración de un sistema de alertas.

Resumiendo, la inteligencia colaborativa es más propia de grupos de trabajo que de grandes masas de personas. Se ve facilitada cuando el objetivo a conseguir o reto a superar se en-

cuenta bien identificado y definido; se realiza una precisa selección de los participantes en el proyecto, en base a sus competencias y habilidades; y se cuenta con las herramientas digitales adecuadas para su desarrollo.

El trabajo de inteligencia requiere **coordinación y colaboración entre personas que tienen diferentes grados de conocimiento, habilidades y experiencia**, ello requiere en ocasiones crear equipos con elementos que manejen distintas disciplinas relacionadas con la inteligencia y en muchos casos organizaciones diferentes.

“Buscamos la integración de agencias y profesionales con diferentes capacidades y hacemos posible una red social de colaboración más amplia y efectiva”

Pedro Cid Sánchez Vizcaíno (CEO TWCI)

SOLUCIONES DE SEGURIDAD E INTELIGENCIA ESTRATÉGICA A NIVEL INTERNACIONAL PARA LAS PYMES. BUENAS PRÁCTICAS

Como ya se ha expuesto a lo largo de esta guía, resulta difícil que una pyme cuente con su propia estructura de seguridad e inteligencia estratégica, por lo que para ello es común recurrir a compañías y/o profesionales especializados que ofrecen esta capacidad.

Así, el objetivo principal consiste en desarrollar productos de inteligencia para ser integrados en soluciones de seguridad e inteligencia estratégica a nivel internacional, mediante el uso intensivo de redes de colaboración humana y del conocimiento e información, una vez validada, analizada y difundida para dar oportuna respuesta a las necesidades de protección de personas y activos en las organizaciones.

Las soluciones aportadas a las pymes se podrían agrupar en cuatro servicios/opciones principales:



Inteligencia, la cual, como ya se ha expuesto supone adquirir el conocimiento necesario que permita orientar nuestra acción, es un factor determinante y clave en toda política de seguridad, ya hablemos del sector público como del privado, así como el desarrollo de negocio en este último –inteligencia competitiva–. Es un producto relacionado con los procesos de toma de decisiones y contribuye de una manera directa a alcanzar una ventaja competitiva.



Seguridad, ya hemos expuesto en esta guía que para entender la seguridad de nuestros días se requiere hacerlo desde un enfoque ampliado, entendiendo que ésta debe de ser abordada desde una perspectiva global en un entorno marcado por la globalización; y, segundo, atendiendo a su dimensión multidisciplinar hay que hacerlo desde los diferentes ámbitos: humano, social, político, medioambiental, económico, o cultural, entre otros. En este nuevo entorno la seguridad debe ser entendida como una actividad y/o función transversal que debe extenderse a toda la organización, generando una sólida cultura de seguridad.



Investigación corporativa, con ella se trata de detectar los posibles delitos que puedan afectar a la organización en su estructura y patrimonio, como el robo y/o pérdida de activos, incursiones no autorizadas en las bases de datos, la mala gestión y fuga de información, competencia desleal o falsificación de capacidades propias por parte de los empleados, por citar algunos de ellos.



Formación, que es considerada como una actividad fundamental para el éxito corporativo de cualquier organización y que debe extenderse a toda la organización. La formación

se contempla en los dos campos, en el de la inteligencia, pues de esta forma se podrá contar con elementos del interior de la organización que faciliten el desarrollo de la inteligencia colaborativa; en el de la seguridad, porque, como ya se ha dicho, ésta incluye a toda la estructura de la organización, además en el proceso de internacionalización de las empresas se requiere disponer de información de todos los desplazados, así como de los propios activos de la empresa.

Estos cuatro servicios/opciones no son soluciones estancas, sino que todos ellos se encuentran relacionados, de manera que las soluciones aportadas incluyan una adecuada combinación de todos ellos en base a las necesidades de la pyme y/u organización correspondiente. En cada uno de ellos se pueden identificar los siguientes productos/opciones u *outputs* diferentes.

ÁMBITO INTELIGENCIA



- **Análisis de riesgos**, para detectar de forma integral las amenazas que generan aquellos que afectan o pueden afectar el desarrollo de la actividad empresarial, garantizando como fin último su resiliencia.
- **Inteligencia geopolítica y geoestratégica**, por una parte, el origen de los riesgos que pueden afectar a una empresa tiene una naturaleza y origen muy variado; además, la globalización, y la consecuente deslocalización de los mercados, ha expandido la actividad empresarial más allá de las fronteras nacionales.
- **Inteligencia criminológica**, orientada al estudio socio criminológico, perfilación criminal y delictología para apoyar a las pymes en sus procesos de selección de personal y, en su caso, en el control de su desempeño profesional.
- **Inteligencia competitiva**, proporciona el conocimiento estratégico sobre el entorno, la actividad del sector, así como los diferentes grupos de interés como socios, competidores, o clientes, entre otros. Facilita enfrentar los procesos de cambio estratégico en la empresa, al orientar oportunamente en los procesos de toma de decisiones, así como influir en la cultura organizacional.

ÁMBITO SEGURIDAD



- **Auditorías**, con este producto se cubren dos objetivos fundamentales: identificar aquellas acciones u omisiones que puedan poner en riesgo la reputación de la empresa y reducir el nivel de sensibilidad y/o vulnerabilidad frente amenazas externas e internas.
- **Gestión de crisis**, entendiendo por tales aquellas situaciones más o menos imprevistas a la que están sujetas todas las organizaciones, las cuales se puede afirmar que, como consecuencia de la globalización y el desarrollo tecnológico, son cada vez más vulnerables.

En consecuencia, uno de los productos a proporcionar a las pymes es precisamente dotarlas del conocimiento y herramientas necesarios para enfrentar este tipo de problemas complejos.

- **Planes, procesos y procedimientos**, como soportes de la organización de todo tipo de corporaciones; mientras que las grandes empresas disponen de departamentos especializados en seguridad que asumen esta responsabilidad, las pymes precisan contratar este tipo de productos que les aportan un valor añadido.
 - Planes, son orientadores de toda organización, con ellos quedan reflejadas las metas, los objetivos y las líneas de acción.
 - Procesos, describen cómo se materializan las líneas de acción de la empresa, constituyen el *know how* de la organización.
 - Procedimientos, determinan los cometidos que realizan los diferentes elementos de la organización para desarrollar las tareas que tienen encomendadas.

ÁMBITO INVESTIGACIÓN CORPORATIVA



- **Due Diligence reputacionales**, implica la investigación de una empresa o persona física, previa a la firma de un contrato u otros negocios.
- **Know you customer (KYC)**, traducido, conoce a tu cliente, producto con el que se trata de proteger la reputación de la organización, evitando quedar vinculados a personas o corporaciones que puedan dañar el prestigio de la empresa.

ÁMBITO FORMACIÓN



- **Apoyar a las pymes en la formación de su personal** en materias relacionadas con la seguridad y la inteligencia. Puede ser considerado como un producto transversal a los anteriores, o bien como un producto específico que responda a un interés puntual de una pyme.
- **Asumir la responsabilidad de la preparación del personal** que, como consecuencia de la internacionalización de la empresa, tenga que desplazarse a zonas de riesgo.

En la ilustración 17 se puede apreciar un resumen de lo expuesto sobre los servicios y productos a los que pueden hoy en día acceder y/o estructurar las pymes como soluciones de seguridad e inteligencia para las mismas.

ILUSTRACIÓN 17. SOLUCIONES DE SEGURIDAD INTERNACIONAL



INTELIGENCIA

- Análisis de riesgos
- Alarmas
- Informes Riesgo País
- Informes Corporativos
- Inteligencia Competitiva



INVESTIGACIÓN CORPORATIVA

- Due Diligence Reputacional
- Know Your Customer (KYC)
- Know Your Partner
- Fraude Interno



SEGURIDAD

- Auditorías de Seguridad Internacional
- Gestión de Crisis
- Planes, Procesos y Procedimientos



FORMACIÓN

- Planes ad hoc Empresas
- Analistas de Inteligencia
- Comités de Crisis

Fuente: Two Worlds Collaborative Intelligence. Elaboración propia

BUENAS PRÁCTICAS

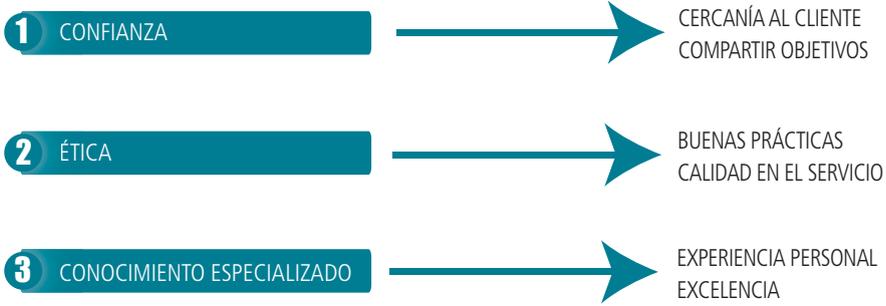
Para hablar de buenas prácticas hay que comenzar haciéndolo de los valores, pues difícilmente ninguna compañía o profesional de seguridad e inteligencia que no esté fundamentado en valores puede aportar las requeridas soluciones de seguridad a las pymes. Aunque podrían enumerarse muchos más se resaltan al menos estos tres: la confianza, basada en primer lugar en compartir los objetivos y metas de la pyme a la que se le van a ofertar las soluciones de seguridad, requiriendo para ello una cercanía y compromiso; la ética, como segundo valor fundamental y en el que se sustentan las buenas prácticas, requiere el compromiso con la calidad en el servicio, la honestidad y la honradez; el conocimiento especializado, para lo cual es fundamental contar con personal con un amplio nivel de conocimientos y experiencia en el sector de seguridad e inteligencia, con una búsqueda constante para alcanzar la excelencia (Ilustración 18).

Otro de los aspectos a considerar en el campo de las buenas prácticas es lo que se conoce como **alianzas estratégicas**. Conscientes de la imposibilidad de abarcar con el necesario conocimiento los diferentes servicios y productos que se ofrecen como soluciones para las pymes se considera necesario, en el marco de la inteligencia colaborativa, alcanzar una serie

“Somos lo que hacemos día a día. De modo que la excelencia no es un acto, sino un hábito”

Aristóteles

ILUSTRACIÓN 18. VALORES



Fuente: Two Worlds Collaborative Intelligence. Elaboración propia

de acuerdos de asociación y apoyo mutuo con compañías punteras en cada uno de los sectores. De esta forma las soluciones ofertadas pueden estar a medida de las necesidades de cada uno de los potenciales clientes.

Son alianzas que en la mayoría de los casos han sido establecidas previamente, creando de este modo un sólido equipo multidisciplinar que abunda en el concepto de inteligencia colaborativa como ya ha quedado explicado en el apartado correspondiente de esta guía.

A continuación, y no con el ánimo de ser exhaustivos, mostramos casos de estructuración de productos/servicios/opciones que pueden surgir al desarrollar el contenido de esta guía; dos de ellos son aportados desde el ámbito de la teoría –pero con el necesario enfoque del conocimiento práctico y experiencia en este ámbito por los autores– y otros cinco son ejemplos reales que han sido desarrollados en algún momento anterior y que pueden ser útiles para entender algunos de los *outputs* finales en todo este proceso y su utilidad/valor añadido para los diferentes usuarios.

CASO 1. CÓMO MONTAR Y ORGANIZAR UNA UNIDAD DE INTELIGENCIA²

Tal y como se ha venido señalando, la inteligencia aplicada a la seguridad ha dejado de ser una disciplina exclusiva de los gobiernos, para pasar a ser también una herramienta de competitividad y seguridad para las empresas. Por ello, las compañías, especialmente las más grandes, se han lanzado a conformar sus propias unidades de inteligencia, a partir de las cuales obtienen el conocimiento necesario para la toma de decisiones.

A continuación, y antes de llegar a las opciones concretas para una pyme, se presentan los condicionantes y factores a tener en cuenta para la creación e integración exitosa de una Unidad de inteligencia (UINT) en una compañía (Rufián, 2019).

No obstante, este ejemplo de estructuración también es muy útil para aquellos proveedores de estos servicios y/o profesionales que deseen diseñar los pasos a seguir por una pyme u otra organización menor, como una solución externa a ellos.

Requisitos de partida

- La dirección responsable de la creación, diseño y recursos de la UINT (humanos, técnicos y económicos) debe tener muy claros los objetivos y servicios que espera obtener de ella. El apoyo y el impulso desde estas instancias son determinantes para el cumplimiento exitoso de las tareas y finalidad de la UINT.
- Capacitación del equipo humano para desarrollar la tarea que se le encomienda. Las personas de la empresa con cometidos de Inteligencia deben tener formación en dicho campo y ser muy conscientes de la importancia de la coordinación entre todos los niveles.
- Cultura de inteligencia en la empresa para asegurar un flujo continuo de información en todos los niveles. En numerosas ocasiones es el factor "humano" el que impide o dificulta establecer una organización para la inteligencia estratégica simple y eficaz.

Cómo integrar la Unidad de Inteligencia en la empresa

El órgano de Inteligencia en una empresa debe estar próximo a la toma de decisiones. De este modo, la integración de la UINT en la estructura empresarial varía en función de los requerimientos de cada empresa. Existen modelos centralizados, descentralizados e híbridos, aunque finalmente será la empresa la que establezca su modelo específico que responda a sus necesidades.

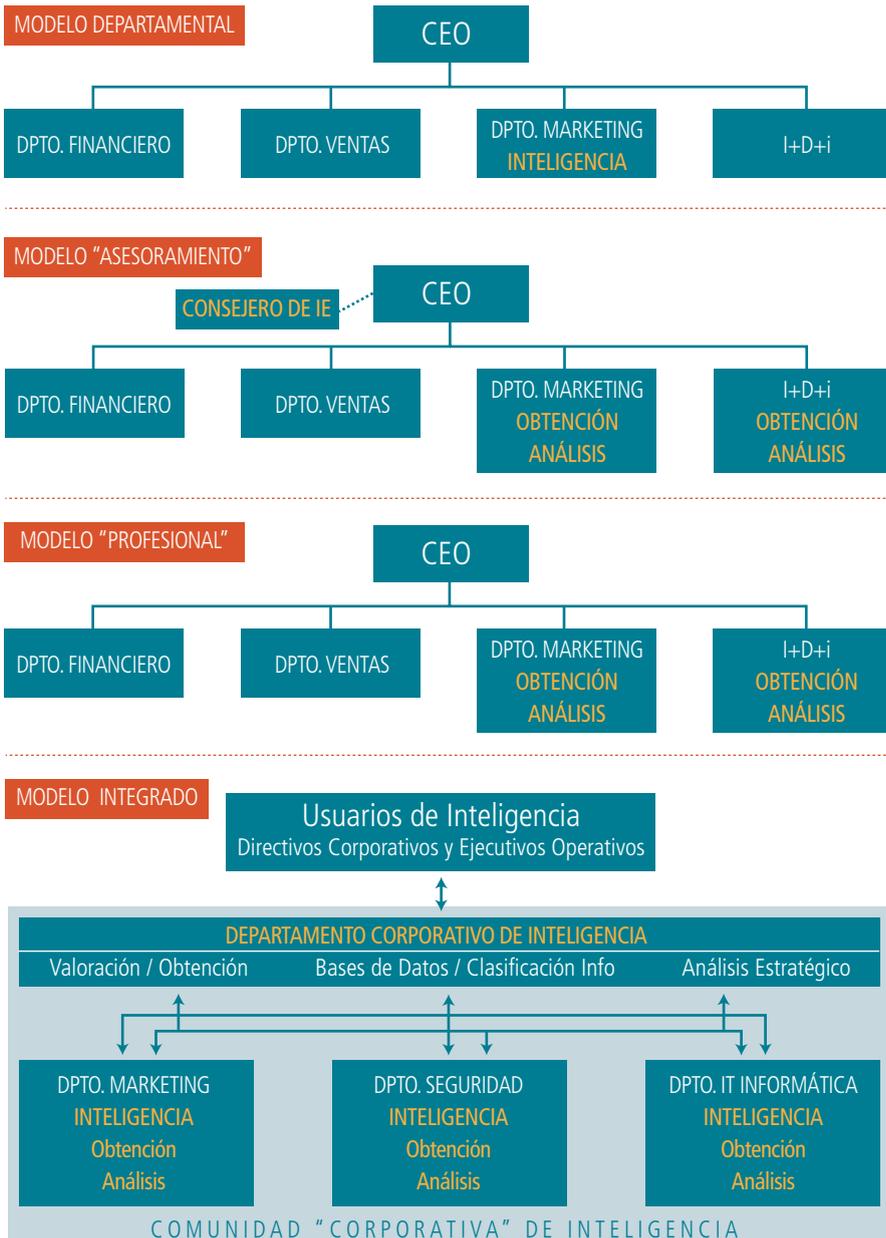
Dependiendo de dónde se sitúe la UINT, si se ubica en compartimentos estancos o no, será capaz de aportar valor integrando al conocimiento generado. Del mismo modo, atendiendo al diseño y en función de ello al funcionamiento de la organización, podrá aportar valor a otras funciones, sin que se produzcan desplazamientos o solapamientos.

Cualquiera que sea la opción elegida, los órganos de inteligencia deben estructurarse de forma que mantengan el debido equilibrio entre las necesidades de inteligencia a nivel estratégico, operacional y táctico.

2. Basado en Rufián (2019).

Algunos ejemplos de modelos de incorporación de la UINT a la empresa se recogen en la ilustración 19.

ILUSTRACIÓN 19. EJEMPLOS DE MODELOS DE INCORPORACIÓN DE LA UINT A LA EMPRESA



Fuente: Elaboración propia

ELEMENTOS CLAVE A CONSIDERAR

- Apoyo de la Dirección
- Formación del personal
- Visión de equipo
- Comunicación
- Tecnologías de la Información
- Asignación/funciones del personal Inteligencia

ORGANIZACIÓN INTERNA DE LA UNIDAD DE INTELIGENCIA

Fases en la implantación:

1. Implicación de la Dirección
2. Designación responsable de Inteligencia
3. Definición del equipo y recursos materiales para la UINT
4. Diagnóstico de Inteligencia (identificar patrones actuales y potenciales para el uso/flujo de la información)
5. Identificación de factores y fuentes de información (factores clave a vigilar, seleccionando las fuentes más relevantes)
6. Definición de productos a generar para los niveles decisores de la empresa.
7. Creación del Manual y Plan de Inteligencia
8. Aplicación de procesos de flujo de información, establecimiento de códigos éticos y de buenas prácticas para que el desempeño de las tareas de la UI de modo autónomo y responsable
9. Seguimiento y revisión de procedimientos

Productos de la UINT:

A continuación, se detallan –adicionalmente o sinónimos de los ya vistos– los productos/*outputs* de una UINT más utilizados:

- Nota informativa
- Informes de inteligencia
- Informes ampliados o suplementos de inteligencia
- Resumen de inteligencia
- Análisis de la situación
- Síntesis informativa
- Informe biográfico o de perfil
- Boletines de noticias/alertas
- *Dashboards*

Estos productos deben tener unos **formatos normalizados de difusión**, que respondan a las necesidades de sus usuarios. Con ello, se consigue que el usuario ahorre tiempo dado que, al estar acostumbrado al mismo formato, puede ir directamente a lo que le interesa. Además, deben ser formatos abiertos a la innovación y a los cambios, en función de las necesidades de los decisores.

CASO 2. BUENAS PRÁCTICAS EN LA RECOGIDA DE INFORMACIÓN

En inteligencia, existe un conjunto de métodos y procedimientos para conseguir los datos y la información necesaria para la toma de decisiones a partir del conocimiento derivado. A continuación, se identifican dos de los métodos con los que cuentan las empresas para incorporar la inteligencia competitiva a su negocio, el OSINT (*Open Source Intelligence*) y el HUMINT (*Human Intelligence*). Ambos han sido seleccionados como buena práctica aplicable por estar entre los más utilizados y valorados en inteligencia.

HUMINT (*Human Intelligence*)

Definición: inteligencia elaborada a partir de información suministrada por personas. Consiste en la obtención de información valiosa de una o más personas, por personal especialmente entrenado para ello, por medio de contacto interpersonal, usando una variedad de tácticas y métodos, tanto activos como pasivos. En definitiva, se trata de personas que obtienen información de otras personas.

Su objetivo final es identificar a las personas que cuentan con información valiosa y conseguir extraer esta información o la colaboración para obtenerla. Es una de las fuentes de inteligencia más antigua y tradicional, llevada a cabo por espías, infiltrados, agentes secretos, informadores, a través de entrevistas, interrogatorios, ...

Qué puede obtenerse a partir de ella: existen diferentes fuentes a partir de las cuales la inteligencia extrae la información que necesita. Pero estas fuentes no pueden proporcionar información sobre cuestiones como las intenciones o la motivación, que permitan a la organización anticiparse a sus competidores o adversarios. Por lo general, este tipo conocimiento sólo puede adquirirse a través de la intervención del personal especializado en técnicas de inteligencia humana (HUMINT).

En el ámbito empresarial, conocer las intenciones de la competencia, así como prevenir posibles fugas internas de información, constituye información valiosa para la planificación y para los procesos de toma de decisiones, y por tanto se traduce en beneficios económicos.

Tipos de actividades HUMINT: los conocimientos y habilidades necesarias para la recolección exitosa de información de fuentes HUMINT requieren llevar a cabo una serie de actividades en función del objetivo de la misión, del entorno y de las fuentes utilizadas.

- **Entrevista:** actividad en la cual una persona facilita, consciente o inconscientemente, información.
- **Interrogatorio:** técnica en la cual el sujeto interrogado no necesariamente colabora para proporcionar la información. Requiere de un interrogador especializado y específicamente capacitado para ello. Adicionalmente, puede requerir la colaboración de personal experto en otras materias (por ejemplo, lingüista).
- **Gestión de contactos y de agentes:** en líneas generales, esta es una actividad en la que se intenta captar personas para obtener información sobre una organización o sobre individuos concretos.
- **Relaciones de enlaces de inteligencia:** consiste en el intercambio de personal entre dos organizaciones, amigas o neutrales, para facilitar el trasvase de información.
- **Vigilancia:** obtención de información sobre personas, lugares o actividades de interés, de manera continua y que se puede prolongar en el tiempo.
- **Reconocimiento:** actividad de obtención de información llevada a cabo de manera puntual sobre determinados puntos o zonas de interés. Al contrario que la vigilancia, el reconocimiento no es continuo en el tiempo.

OSINT (*Open Source Intelligence*)

Definición: las fuentes de información OSINT se refieren a toda la información desclasificada, de acceso público y gratuito. Ello significa que no pueden contener información clasificada, ni proceder de fuentes cerradas a las que se accede a través de pago (la inteligencia elaborada a partir de información que no es pública y no está disponible en internet se considera *NO-SINT-Non Open Source Intelligence*).

Qué puede obtenerse a partir de ellas: OSINT permite obtener datos de personas y de organizaciones que han sido expuestos públicamente. Por ejemplo, muchos individuos comparten gran parte de su información personal por internet y las redes sociales, que puede encontrarse, recogerse y organizarse con esfuerzo y las herramientas y el conocimiento adecuados.

Dónde encontrarlas: la mayoría de la información se puede encontrar en internet. La principal dificultad radica en identificar la fuente correctamente, y a partir de allí, filtrar los datos en función de las necesidades de información. Para ello, en la mayoría de los casos, es necesario contar con herramientas especializadas y el apoyo de expertos.

Actualmente es tal la cantidad de información a la que, con mayor o menor facilidad, se tiene acceso que no sólo es necesario encontrar la que sea de interés empresarial, sino que, además, hay que ser capaz de dominar esa ingente cantidad de datos que puede llevar al decisor a perder la perspectiva, convirtiéndose en un problema.

- **Informe de situación.** Con la antelación necesaria se debe preparar un informe país en el que además de la situación socio política y de seguridad del lugar de destino, se incluyen una serie de recomendaciones al viajero y los indicadores pertinentes. Es un informe personalizado y ejecutivo en el que se incluyen también contactos y localizaciones de puntos de interés y servicios.
- **Atención médica a desplazados.** A través de una compañía especializada a nivel global, se oferta este servicio que cuenta con una cobertura global.
- **Apoyo de seguridad.** La utilización de una herramienta de geolocalización y respuesta 24/7 permite mantener localizado al viajero y alertarlo de los peligros potenciales u otras incidencias que pudieran afectar a su seguridad, así como los contactos necesarios con las autoridades locales. Asimismo, y en el caso de un grave deterioro de la situación de seguridad, se dispone de herramientas para la evacuación a un punto seguro y posterior repatriación del personal.
- **Formación.** Se aportan para cada caso los correspondientes planes de formación individualizada para viajeros frecuentes y expatriados, en base a su perfil y nivel de riesgo y siempre alineados con los criterios organizativos de la empresa.

CASO 4. ANÁLISIS DE RIESGOS PARA EL DESARROLLO DE UN PROYECTO

Con este caso, podemos valorar el producto obtenido y sus posibles aplicaciones para casos similares. Solicitado por una empresa energética que pretendía llevar a cabo la construcción de un parque eólico *off shore* en un país exterior, se preparan una serie de informes mediante el análisis de fuentes abiertas (OSINT) y monitorización de redes sociales que permitieron identificar a las organizaciones y personas opositoras al proyecto, así como informar anticipadamente de sus intenciones de llevar a cabo manifestaciones, o convocatorias de ruedas de prensa, entre otras, con la intención de paralizar el proyecto.

También permitió la identificación de las principales demandas de la población y sectores afectados, lo que facilita que la empresa tome medidas para mitigar este tipo de percepciones y en su caso reacciones y con ello potenciar su reputación, algo fundamental para proteger la marca y aumentar las opciones de negocio.

Posteriormente, la empresa/profesionales de seguridad que realizan los informes iniciales, es conveniente que monitoricen el desarrollo del proyecto para detectar cualquier tipo de riesgo que afecte al inicio de las obras. No hay que olvidar que este tipo de retrasos pueden llegar a suponer importantes pérdidas económicas para la organización.

CASO 5. ANÁLISIS DE RIESGOS

Es este un modelo que permite la detección anticipada de incidentes de seguridad que puedan afectar a la actividad comercial de una empresa.

En primer lugar, se trata de alertar sobre el grado de seguridad del lugar dónde la empresa pretende desarrollar su actividad comercial. Para ello se ha realizado un estudio de riesgo-país en más de cien países en base a fuentes abiertas y agencias de inteligencia. Lo anterior ha permitido construir un *risk rating* de 176 países, clasificándolos en cinco niveles de riesgo (muy alto, alto, medio, bajo y muy bajo), atendiendo a la estabilidad del país, sus condiciones sanitarias y su situación de seguridad.

Como continuación a este informe inicial de riesgos se proporciona un sistema de alertas globales de eventos de seguridad que permiten tener una visión general de la situación. Además, el sistema permite que cada cliente/empresa pueda introducir un sistema de alertas corporativas en base a sus intereses particulares ya sean por el tipo de actividad o por el lugar en el que se van a realizar.

Este tipo de productos de seguridad es posible mediante la concurrencia entre la empresa de seguridad con empresas especializadas en inteligencia económica, generación de alertas y geolocalización, es decir las "alianzas estratégicas" que anteriormente comentábamos.

CASO 6. ACTIVIDADES DE DUE DILIGENCE

A requerimiento de una institución financiera de un país latinoamericano, se localizó a través de OSINT y SOCINT a una empleada de un país europeo que había abandonado el país y regresado a su país con una deuda frente a dicha entidad de 60.000 €.

Esta persona fue localizada en su nuevo domicilio en el país europeo e informada la institución financiera para que pudiera actuar a través de las autoridades pertinentes.

CASO 7. PLANES DE SEGURIDAD

A petición de un exclusivo centro residencial y campo de golf de una ciudad latinoamericana, que había tenido varios casos de incursión y robo en viviendas, se llevó a cabo una auditoría para, en base a ella, presentar un plan de seguridad integral y su correspondiente programa de implementación.

Como una de las primeras medidas se nombró un nuevo jefe de seguridad, modificándose el concepto de seguridad, poniendo un mayor énfasis en los aspectos tecnológicos.

Esta actividad supuso la colaboración con tres empresas de diferentes ámbitos de actividad: riesgos laborales, seguridad física y seguridad de sistemas. Por otra parte, se impulsó un acercamiento a las autoridades locales para una mayor implicación en garantizar la seguridad de la instalación y las personas que habitan y trabajan en ella.

A MODO DE SÍNTESIS

El objetivo principal de esta guía radica en concienciar al sector empresarial, así como a otras organizaciones, y en particular a sus directivos, de la importancia que tiene incorporar la inteligencia a los procesos de las organizaciones. Así como mostrar a los profesionales interesados en este campo de actividad el contenido, procesos y *outputs*, de gran utilidad para la pyme, que se pueden generar desde esta parcela de conocimiento.

Hoy en día, gracias al impresionante desarrollo tecnológico disponemos de un gran volumen de información que, sin embargo, por sí mismo no representa ningún valor añadido. La superioridad informativa la debemos entender como la disponibilidad en tiempo oportuno y de forma precisa de la información debidamente tratada y analizada, es decir de la inteligencia. Solamente de esta manera se alcanzará la verdadera ventaja competitiva.

Cuando hablamos de seguridad se debe tomar en consideración una idea clave, cual es que su finalidad última es la supervivencia de la organización y por tanto es un elemento fundamental de la cadena de valor de cualquier empresa, con independencia de su tamaño, siendo precisamente la inteligencia una herramienta fundamental para garantizar la seguridad.

La seguridad plena es imposible, por ello es necesario plantearnos tres preguntas fundamentales:

- **¿qué tenemos que proteger?**, nos dirá el objetivo de la seguridad;
- **¿de qué nos tenemos que proteger?**, analiza los riesgos a los que nos enfrentamos; y
- **¿cómo nos protegemos?**, para así determinar los medios y estrategias a aplicar.

Si llevamos esta conceptualización de la seguridad al mundo empresarial, vemos que, como estado, la seguridad trata de proteger a las personas, las infraestructuras, la marca, la reputación y la continuidad de negocio. Como situación, requiere de un exhaustivo y continuo análisis de riesgos y amenazas que le permitan anticiparse a una situación perjudicial para sus intereses, lo que entre otros aspectos aconseja disponer de un adecuado sistema de inteligencia. Como acción, toda empresa deberá tener su plan de seguridad, su plan de continuidad de negocio, así como los necesarios planes de contingencia y tener previsto para cada uno de ellos los medios pertinentes para garantizar el fin último que ya hemos dicho que es la propia supervivencia de la empresa. Desde la perspectiva de la seguridad como función, debe ser entendida como un proceso transversal que afecta a los diferentes departamentos, pero que debe de ser dirigido y/o impulsado desde el más alto nivel de la organización.

Además de conocer nuestras propias fortalezas y debilidades, se precisa conocer las oportunidades y amenazas que conforman el contexto en el que desarrollamos nuestra actividad empresarial. La inteligencia es pues la herramienta capital que nos va a facilitar la información precisa sobre los procesos internos, así como del contexto externo, permitiendo con ello alcanzar una posición de ventaja en la toma de decisiones.

Las empresas, como organizaciones cuya actividad se desarrolla en un escenario complejo e incierto precisan contar con una superioridad de la información, a la cual se llega precisamente mediante la inteligencia, y que puede ser considerada como un mercado/actividad en alza, porque las empresas necesitan de esta función más que nunca. La parte positiva a esta necesidad es que hoy en día esta función se ve facilitada por el desarrollo de las nuevas tecnologías, lo que facilita la interconexión y la cooperación, lo que da sustento al concepto de inteligencia colaborativa. Ésta permite alcanzar grandes objetivos con unos medios reducidos y a un coste asumible por la mayoría de las organizaciones empresariales.

Las necesidades de inteligencia de las empresas se podrían agrupar en dos grandes bloques, la inteligencia competitiva (IC) y la inteligencia para la seguridad.

La inteligencia es en sí misma proactiva y reconoce que la ausencia de acontecimientos dramáticos no asegura una ausencia de amenazas competitivas, estando orientada, en consecuencia, a la detección de señales de alerta y a la prevención de riesgos.

La competitividad de una organización es fundamental a la hora de realizar el análisis estratégico que nos determine los objetivos a alcanzar, así como identificar nuestros principales competidores y colaboradores.

Los cambios organizativos son una de las tareas más complejas a las que se enfrenta una organización, máxime si el cambio viene motivado por un agente externo, como podría ser la situación de algunas pymes tras la COVID-19. Para el diseño estratégico es capital la concurrencia de la inteligencia competitiva, especialmente si se trata de cambios estructurales, así como hacer uso de la denominada inteligencia colaborativa.

Destacando que las dos señas de identidad de la inteligencia colaborativa son: compartir el conocimiento y apoyar la toma de decisiones. **La inteligencia colaborativa se mueve en el campo de las tecnologías sociales y su razón de ser es apoyar los procesos de toma de decisiones.** Sobre la primera de ellas debemos tener en cuenta que cuanto más compartamos más tendremos. El mercado requiere respuestas rápidas y con experiencia y para ello se precisa compartir conocimientos. En relación con la segunda, es necesario tener en cuenta que hoy más que nunca vivimos en un mundo global y digital donde las tecnologías de la información avanzan a pasos agigantados, empieza a ser necesario potenciar la inteligencia colaborativa para conseguir compañías inteligentes, capaces de adaptarse a cualquier cambio y necesidad. Y además hay que poner el énfasis en que las tomas de decisiones se producen, hoy más que nunca, en un entorno complejo y cambiante, por lo que se precisa una inteligencia oportuna y precisa.

Como soluciones para las pymes, se han de desarrollar productos de inteligencia para ser integrados en soluciones de seguridad a nivel internacional, mediante el uso intensivo de redes

de colaboración humana y del conocimiento e información, una vez validada, analizada y difundida para dar oportuna respuesta a las necesidades de protección de personas y activos en las organizaciones.

Las soluciones aportadas a las pymes se agrupan en cuatro productos, *outputs* y/o servicios principales: **inteligencia, seguridad, investigación corporativa y formación**. Estos cuatro *outputs* no son soluciones estancas, sino que todos ellos se encuentran relacionados, de manera que las soluciones aportadas incluyan una adecuada combinación de todos ellos en base a las necesidades del usuario. En cada uno de ellos se ofertan diferentes opciones, con valor añadido para una pyme u organización.

Asimismo, es importante destacar que al hablar de buenas prácticas hay que comenzar haciéndolo de **valores**, pues difícilmente ninguna compañía y/o profesional de seguridad e inteligencia que no esté fundamentado en valores puede aportar las requeridas soluciones de seguridad e inteligencia estratégica a una pyme u otra organización. Aunque podrían enumerarse muchos más, se resaltan al menos estos tres:

- confianza, basada en primer lugar en compartir los objetivos y metas de la pyme u organización a la que se le van a desarrollar las soluciones de seguridad, requiriendo para ello una cercanía y compromiso;
- ética, como segundo valor fundamental y en el que se sustentan las buenas prácticas, requiere por tanto el compromiso con la calidad en el servicio, la honestidad y la honradez;
- conocimiento especializado, para lo cual es fundamental contar con personal con un amplio nivel de conocimientos y experiencia en el sector de seguridad e inteligencia, con una meta de crecimiento constante en este ámbito para alcanzar la excelencia.

Conscientes de la imposibilidad de abarcar con el necesario conocimiento los diferentes servicios y productos que se pueden ofrecer o desarrollar como soluciones para las pymes se considera necesario, en el marco de la inteligencia colaborativa, alcanzar una serie de acuerdos de asociación y apoyo mutuo con compañías punteras en cada uno de los sectores. De esta forma las soluciones ofertadas pueden estar a medida de las necesidades de cada uno de los potenciales usuarios.

En definitiva, con este trabajo se ha pretendido establecer una guía clara para que las pymes y otros interesados puedan ser conscientes de que **la necesidad de inteligencia estratégica y seguridad no es algo exclusivo de las grandes empresas** y va más allá de lo que entendemos tradicionalmente como seguridad, pudiendo ser necesario para cualquier empresa u organización con independencia de su tamaño o sector. Hoy en día tenemos un claro ejemplo de lo importante que es haber pensado en la estrategia de seguridad e inteligencia empresarial, los riesgos que está suponiendo la pandemia originada por la COVID-19.

Por ello, pretendemos en este texto:

- Aclarar qué es la seguridad e inteligencia estratégica, y por qué afecta claramente, y cada vez más, también a las pymes.
- Analizar el nuevo escenario geoestratégico al que nos enfrentamos, y así también la actividad empresarial, con todos los aspectos que es necesario tener en cuenta a la hora de determinar la situación del entorno empresarial.
- Definir el concepto de seguridad ampliada, de forma que claramente se pone de manifiesto cómo afecta a cualquier empresa u organización, y concretamente a las pymes.
- Resaltar que cuando una empresa se internacionaliza es aún si cabe más necesario abordar el ámbito de su inteligencia y seguridad, y cuáles son los aspectos que abarca.
- Poner de manifiesto que el propio negocio desarrollado por la pyme puede tener claras debilidades y amenazas y no ser seguro, lo que se puede prever con un análisis previo e inversión en seguridad e inteligencia. Y en el mismo sentido, plantear si el negocio es competitivo desde el punto de vista de la inteligencia competitiva.
- Definir la inteligencia colaborativa, sus bondades, su aplicación, su necesidad, ante el entorno global en el que se desenvuelve la actividad empresarial, y también las pymes.
- Concluir mostrando unos ejemplos de buenas prácticas, en los que la seguridad e inteligencia han resultado de gran utilidad a las empresas, que permiten concretar en situaciones reales todos los conceptos que se han introducido a lo largo de esta guía.

“Hoy en día el mundo es una oportunidad de negocio, no debemos dejar de mejorar y ser productivos porque nuestro entorno de seguridad sea complicado. Complicado también lo es el mundo y no por eso deja de girar ... «proteger es rentable»”

CEO TWCI

ACRÓNIMOS

BI - *Business Intelligence*

CI - *Competitor Intelligence*

DAFO - Análisis de debilidades, amenazas, fortalezas y oportunidades

ES - *Enviromental Scanning*

FM - Fondo Monetario Internacional

HUMINT - Inteligencia Humana (*Human Intelligence*)

IC - Inteligencia Competitiva

IE - Inteligencia Económica

IES - Inteligencia Estratégica

IMINT - Inteligencia de imágenes (*Imagery Intelligence*)

IT - Inteligencia Tecnológica

KYC - Conoce a tu cliente (*Know Your Customer*)

NO-SINT - Inteligencia de fuentes no abiertas (*Non Open Source Intelligence*)

OSINT - Inteligencia de fuentes abiertas (*Open Source Intelligence*)

PESTLE - Análisis de factores políticos, económicos, sociales y tecnológicos (*Political, Economic, Social, Technological, Legal and Environmental analysis*)

PIB - Producto Interior Bruto

SIGINT - Inteligencia de señales (*Signals Intelligence*)

SCIP - *Society of Competitive Intelligence Professional*

SOCMINT - Inteligencia de redes sociales (*Social Media Intelligence*)

TWCI - *Two Worlds Collaborative Intelligence*

UINT - Unidad de Inteligencia

BIBLIOGRAFÍA

BAI Agencia de Innovación (2008). *Modelos de vigilancia tecnológica e inteligencia competitiva*.

Bergeron, P. y Hiller C.A. (2002). Competitive Intelligence. *Annual Review of Information Science and Technology* (ARIST02), Vol. 36. Blaise Cronin, Editor. Asis&E.

Cavaller, V. (2009). Actualidad de la inteligencia competitiva. *Cuadernos de inteligencia competitiva, vigilancia estratégica, científica y tecnológica*, Vol. 2, Edición 1, pp. 31-44.

Clark, R. M. (2017). *Intelligence Analysis*. CQ Press.

Collins, A. (2016) *Contemporary Security Studies*. Oxford.

García Alsina, M. (2011). Tesis doctoral: *Contribución de la inteligencia competitiva en el proceso de adaptación al EEES: el caso de las universidades españolas*, defendida el 10 de Julio de 2011.

Gilad, B. (1992). What you don't know, can hurt you: formalising competitive intelligence activities. *Journal of AGSI*.

Gilad, B. (2015). "Competitive Intelligence" Shouldn't Just Be About Your Competitors. *Harvard Business Review*. Recuperado de: <https://hbr.org/2015/05/competitive-intelligence-shouldnt-just-be-about-your-competitors>.

Hackman, J. R. (2011) *Collaborative Intelligence*. Berrett-Koehler Publishers.

Izquierdo, H. (2018). *La inteligencia competitiva en los países del entorno de competencia de España*. En <http://www.seguridadinternacional.es/?q=es/content/la-inteligencia-competitiva-en-los-pa%C3%ADses-del-entorno-de-competencia-de-espa%C3%B1>.

Izquierdo, H. (2019). *Inteligencia económica y competitiva en grandes empresas españolas*. Comité de Reflexión sobre Internacionalización, Club de inversores y exportadores.

Larribar Hinojar, B. y González Cussac, J. L. (2011) *Inteligencia económica y competitiva*. Tirant Lo Blanch.

Markova, D. y McArthur, A. (2015) *Collaborative Intelligence*. Spiegel & Grau.

Mesias (2018). *Inteligencia Económica y Competitiva: Una necesidad estructural para la competitividad de España en un mundo globalizado. Informe Cero*. Observatorio MESIAS de Inteligencia Económica y Competitiva. Informe MESIAS. Ed. MESIAS - Inteligencia de Marca España. Madrid. España.

Ortoll, E. y García, M. (2015) *La Inteligencia Competitiva*. Editorial UOC.

Porter, M. (2004). *Competitive Strategy. Techniques for analyzing industries and competitors*. Simon and Schuster New York.

Rufián Albarrán, M. (2019). *Unidad de inteligencia*. En Postgrado de Inteligencia Económica y Seguridad, llevado a cabo por Universidad Pontificia de Comillas ICAI-ICADE.

Sánchez (2015). La toma de decisiones en la empresa ante la incertidumbre política. El papel de la Inteligencia Económica/Empresarial. *Papeles de Liderazgo*, nº 8. Septiembre.

Shepherd, L. (2013). *Critical Approach to Security*. Routledge.

Zanoni, A. (2012). *Strategic Analysis*. Routledge.

EDITAN: CONSEJO GENERAL DE ECONOMISTAS DE ESPAÑA y CÁMARA DE COMERCIO DE ESPAÑA

ISBN: 978-84-86658-98-4

No está permitida la reproducción total o parcial de este estudio, ni su almacenamiento o transmisión por ningún medio (electrónico, mecánico, grabación, fotocopia, etc.) sin permiso previo del editor.

Diseño y maquetación: desdezero, estudio gráfico



ESTUDIOS

5

GUÍA SOBRE SEGURIDAD E INTELIGENCIA ESTRATÉGICA PARA PYMES

Una guía que orienta sobre la necesidad de la inteligencia y seguridad en los procesos de internacionalización de las pymes

DICIEMBRE 2020

COLABORADORES

 **economistas**
Consejo General
EC *economistas contables*

CÁTEDRA EC-CGE 

 **economistas**
Consejo General
empresa

economistas
Consejo General

Cámara
de Comercio de España

 **TWCI**