FUNDACIÓN ESYS EMPRESA, SEGURIDAD Y SOCIEDAD

EL GRADO DE MADUREZ DEL SISTEMA DE GESTIÓN DE SEGURIDAD CORPORATIVA:

Caso de estudio en empresas del IBEX basado en Enterprise Security Risk Management (ESRM)

Jose Márquez

Global Head Security Risks & Resilience.

Naturgy Energy Group.

PhD Candidate (Universidad Rey Juan Carlos).

Abstract La globalización y la hiperconectividad afectan a la resiliencia organizacional con amenazas como la reciente pandemia de COVID-19 o ciberataques a gran escala. Para fortalecer las capacidades de resiliencia organizacional, es necesario un marco como el modelo internacionalmente reconocido COSO-ERM, que permita la gestión integral de los riesgos. En este estudio se analiza el modelo de gestión la función de seguridad corporativa en grandes empresas que cotizan en la bolsa española. Para ello se ha utilizado el modelo ERMsec ©, alineado con la Guía ESRM de ASIS International y otras normas internacionales, por resultar adaptable a cualquier tipo de organización y compatible con su respectivo sistema integrado de gestión. Entre otras conclusiones, resulta relevante para próximos estudios identificar y analizar desde la perspectiva de la gestión estratégica, la gobernanza organizacional y el cumplimiento (responsabilidad de los comités de dirección y consejos de administración) a través de un programa de ESRM, así como las implicaciones gerenciales de la función de seguridad corporativa y su capacidad para promover el compromiso de la alta dirección y los grupos de interés.

Keywords Enterprise Security Risk Management – Resiliencia Organizacional - Security Management System - Crisis Management – Gobierno Corporativo.

INDICE

1. INTRODUCCIÓN.

2. ANTECEDENTES.

3. MARCO TEÓRICO.

3.1 Resiliencia Organizacional.

3.2 Enterprise Risk Management (ERM).

3.3 Enterprise Security Risk Management (ESRM).

3.4 Sistema de Gestión.

3.5 Modelos de sistemas de Gestión de Seguridad.

3.6 Sistemas integrados de gestión.

3.7 Justificación del modelo propuesto.

3.8 Estructura del modelo ERMsec ©.

4. METODOLOGÍA.

4.1 Identificación del problema.

4.2 Determinación del diseño de investigación.

4.3 Especificación de las hipótesis.

4.4 Definición de las variables.

4.5 Selección de la muestra.

4.6 Diseño del cuestionario.

4.7 Organización del trabajo de campo.

4.8 Obtención y tratamiento de los datos.

5. RESULTADOS DEL ANÁLISIS.

5.1 Datos Generales

5.2 Sistema de Gestión

6. DISCUSIÓN.

7. CONCLUSIONES.

8. BIBLIOGRAFÍA.

1.

INTRODUCCIÓN

Tradicionalmente, la gestión de riesgos en las empresas ha estado descoordinada y aislada en silos (Mcshane, Nair & Rustambekov, 2011). Sin embargo, en las últimas décadas el nuevo entorno Volátil, Incierto, Complejo y Ambiguo (V.U.C.A.), en el que las organizaciones desarrollan actividades, ha generado la necesidad de adaptar e implementar un nuevo marco estratégico para la gestión de riesgos. En este escenario, el modelo más extendido y aceptado es el denominado Enterprise Risk Management (ERM), que contribuye de manera coordinada a la resiliencia organizacional.

Algunos de los riesgos a los que se enfrentan las organizaciones son los relacionados con la gestión de la seguridad corporativa. Dicha gestión debe estar integrada con la estrategia general de riesgos de la organización junto con las demás áreas corporativas y de negocio, e incluso la alta dirección y otros departamentos participan activamente (Nalla, Morash, 2002). Desde la perspectiva estratégica, las empresas y sus líderes deben comprender y promover que los diferentes individuos y grupos dentro de la organización son propietarios y responsables de su riesgo (Bromiley et al., 2015). Desde sus inicios, la función de seguridad corporativa (en adelante, security) en las organizaciones se ha centrado en el rol de gestionar directamente los riesgos antisociales intencionados que pueden afectar al negocio, incluso brindando apoyo transversal durante la gestión de crisis con el fin de minimizar el impacto (Ludbey, Brooks & Coole, 2018).

En los últimos años, importantes asociaciones de profesionales y gerentes de seguridad a nivel mundial han progresado más allá de la simple convergencia de la seguridad (seguridad física y ciberseguridad) y han trabajado en un nuevo modelo holístico alineado con ERM (Johnson, Spivey, 2008), llamado Enterprise Security Risk Management (en adelante ESRM).

Hoy en día, los directores ejecutivos han entendido que el logro de los objetivos de las empresas depende de cómo gestionan estratégicamente los riesgos (Hoyt, Liebenberg, 2011); por lo tanto, incorporar ESRM como parte del marco de ERM se vuelve vital, particularmente en grandes organizaciones y empresas multinacionales. Por tanto, conviene estudiar empíricamente la contribución real de Security en agregar valor a las organizaciones (Gill, 2007), especialmente en su capacidad de resiliencia, tomando como marco ESRM y otros estándares internacionales.

Security, además de gestionar los riesgos operacionales antisociales de las organizaciones, colabora activamente tanto en la obtención y análisis de la información de inteligencia que recibe la alta dirección para la toma de decisiones estratégicas (Crump, 2015), como en el liderazgo transversal de la gestión de crisis en el ante eventos perturbadores graves (pandemias globales, desastres naturales, ciberataques a gran escala, etc.). Según Petruzzi y Loyear (Petruzzi, Loyear, 2016a), ESRM impulsa a todas las partes del negocio a reconocer y tratar proactivamente el riesgo, sin pasar por alto que la alineación de la continuidad del negocio y la gestión de crisis dentro de la filosofía de ESRM son un requisito clave en cualquier programa de resiliencia. Actualmente el

concepto de “seguridad” es entendido, en sus dimensiones de “estado o situación” y de “proceso”, y contribuye a reducir el riesgo y proteger o desarrollar resiliencia contra posibles escenarios de amenazas (Jore, 2019).

Por lo tanto, este estudio sirve como base para futuras investigaciones sobre la contribución real a la resiliencia organizacional de un sistema de gestión de seguridad basado en ESRM, tanto por los riesgos específicos de seguridad como en su labor de liderazgo de los procesos transversales de gestión de crisis. Se han realizado estudios previos en ESRM sobre modelos de gobernanza para riesgos de seguridad, basados en la composición de comités o grupos de trabajo (Allen, Brian et al., 2018); pero desde la perspectiva de la gestión estratégica, se ha observado una gap en la definición de un modelo específico en el que determinar la madurez de un sistema de gestión de la seguridad vinculado con la gobernanza organizacional y el cumplimiento (responsabilidad de los comités de dirección y consejos de administración) a través de un programa de ESRM. Por esta razón es necesario profundizar en un modelo de madurez de seguridad alineado con la Guía ESRM (ASIS International) y otros estándares internacionales, que debe ser flexible para cualquier tipo de organización y compatible con su sistema integrado de gestión de riesgos y de resiliencia.

2.

ANTECEDENTES

La misión de la Fundación ESYS - Empresa Seguridad y Sociedad (en adelante, ESYS) es generar un ámbito interdisciplinario sobre temas relacionados con seguridad y empresa, mediante estudios de investigación, foros de divulgación, actividades de formación, y creación de una base documental amplia.

En el desarrollo de su tesis doctoral, el investigador y responsable de este proyecto ha elaborado un modelo de madurez del sistema de gestión de security, tomando como referencia entre otros, el estándar **"Enterprise Security Risk Management"** (ESRM) desarrollado por la Commission on Standards and Guidelines de ASIS International. El objetivo de dicha investigación es estudiar la contribución real a la resistencia organizacional de un sistema de gestión de seguridad basado en ESRM. Por este motivo sería deseable contar con un modelo de madurez de seguridad alineado con la Guía ASIS ESRM y otros estándares internacionales, que debería ser flexible para cualquier tipo de organización y compatible con dicho sistema integrado de gestión de riesgos.

Esa investigación incluye un marco teórico para establecer este modelo y, en consecuencia, también parece relevante identificar y analizar las implicaciones gerenciales de la función de seguridad corporativa y su capacidad para promover el compromiso de la alta dirección y los grupos de interés.

A partir de este nuevo modelo se ha elaborado un cuestionario basado en el sistema Capability Maturity Model Integration (en adelante CMMI) desarrollado por la Universidad Carnegie Mellon, y que establece 5 niveles de madurez de los procesos.

La encuesta se realizó de forma anonimizada entre algunas de las principales empresas del país, con un método que garantizará la fiabilidad y calidad de los datos aportados.

El objetivo principal es evaluar el nivel de madurez del sistema de gestión de Security con respecto a estándares reconocidos internacionalmente, con un modelo que permita visualizar su evolución en próximos estudios. También se pretenden otros objetivos secundarios como estudiar la posición del director de seguridad en la jerarquía de la organización y la gestión de riesgos de security en particular, así como las necesidades de formación o la inclusión de la disciplina de inteligencia dentro de los procesos de security. Será interesante a futuro utilizarlo como base para explorar las implicaciones de los consejos de administración y dirección de las organizaciones en la gestión de riesgos derivados de las amenazas de seguridad, y su influencia en el gobierno de la resiliencia organizacional.

3.

MARCO TEÓRICO.

3.1.

Resiliencia Organizacional

El concepto de resiliencia ha sido usado en el pasado tanto en las áreas de psicología o ecología, y en los últimos años se ha extendido su uso en múltiplex contextos, convirtiéndolo en una expresión de moda, con la percepción de ser un atributo positivo de una organización, objeto o sistema (Martin, Sunley, 2015).

En cuanto a su normalización, la relación directa de la seguridad con la resiliencia organizacional se ha observado en la creación en 2015 del comité ISO / TC 292 por la Organización Internacional de Normalización (ISO). Entre sus objetivos se encuentran la estandarización de capacidades, la seguridad organizacional y la gestión de la resiliencia. De acuerdo con ISO 22316:2020 'Seguridad y resiliencia - Resiliencia organizacional - Principios y atributos', la resiliencia organizacional se define como "la capacidad de una organización para absorber y adaptarse en un entorno cambiante" para poder alcanzar sus objetivos. sobrevivir y prosperar. De acuerdo con este estándar, las organizaciones más resilientes pueden anticipar y responder a las amenazas y oportunidades que pueden resultar de cambios repentinos o graduales en sus contextos internos y externos. Mejorar la resiliencia debe ser un objetivo organizacional estratégico y es el resultado de buenas prácticas comerciales y una gestión de riesgos eficaz.

La actividad empresarial está intrínsecamente sujeta a riesgos para la consecución de objetivos, independientemente de la naturaleza de la actividad, volumen de negocio o área geográfica de la operación. La exposición y gestión de esos riesgos condicionan la capacidad de maximizar el valor, por lo que los resultados obtenidos varían en función de la gestión de dichos riesgos. Eastburn y Sharland (Eastburn, Sharland, 2017) establecieron en su investigación cómo un proceso de gestión de riesgos eficaz podría ser una solución para maximizar las oportunidades de riesgo / recompensa.

Muchas empresas operan actualmente en un entorno V.U.C.A., que dificulta a los líderes la realización de diagnósticos de riesgo fiables, necesarios para la toma de decisiones; asignar los recursos adecuados para proteger a la empresa de riesgos negativos; e identificar oportunidades (Bennett, Lemoine, 2014). Las organizaciones empresariales perciben la incertidumbre como el mayor riesgo que amenaza el logro de los objetivos. Por lo tanto, necesitan un marco de gestión que les ayude a mitigar todos los riesgos conocidos y emergentes antes de que ocurran (Gupta, 2016). Entre todos los riesgos posibles, se destaca el impacto extremo de eventos impredecibles e improbables, llamados 'cisnes negros' (Taleb, 2007). Aunque no existe un sistema de gestión de riesgos infalible para prevenir la ocurrencia de esos cisnes negros, la implementación del sistema puede ayudar a respaldar los procesos de toma de decisiones sobre las medidas que deben implementarse para mitigar el impacto en la organización.

3.

MARCO TEÓRICO.

3.2.

Enterprise Risk Management (ERM)

Si bien a finales de la década de 1980 ya existía un trabajo incipiente en este campo, el marco de gestión de riesgos basado en ERM apareció en la década de 1990 como resultado de una necesidad derivada de un entorno competitivo y complejo, buscando vincular la gestión de riesgos con las actividades de las empresas (Arena, Marika, Arnaboldi & Azzone, 2010). ERM es la forma principal adoptada por las empresas que realizan crecientes esfuerzos para organizar la incertidumbre, que alcanzó su punto máximo en esa década (Shetty et al., 2018). Según Govender (Govender, 2019), Australia y Nueva Zelanda fueron los primeros países en desarrollar un modelo holístico de gestión de riesgos en 1999 a través del estándar AZ / NZS 4360. Los escándalos financieros de años posteriores y el colapso de grandes empresas multinacionales como Enron y Worldcom hicieron necesario introducir estándares regulatorios para evitar el fraude y el riesgo de quiebras, como la Ley Sarbanes-Oxley de 2002.

En 2004, el Comité de Organizaciones Patrocinadoras de Treadway (COSO) publicó la primera guía completa de ERM (COSO ERM — Marco Integrado de Gestión de Riesgos Empresariales). Este estándar se actualizó en 2017 para guiar la integración de ERM hacia el establecimiento de estrategias y desempeño (Prewett, Terry, 2018). Bharathy y

McShane (Bharathy, McShane, 2014) proponen la implementación de ERM utilizando un enfoque que permite la implementación efectiva de la gestión de riesgos empresariales y la gestión de riesgos estratégicos complejos a través de la norma de gestión de riesgos ISO 31000:2018.

Tener un marco de gestión de riesgos implementado no significa que se pueda confiar en él y que las empresas se puedan acostumbrar a él. Si retrocedemos en el tiempo y observamos el efecto negativo en la economía mundial de las 'hipotecas subprime' en 2008, podemos ver que las empresas con la gestión de riesgos más sofisticada (por ejemplo, los bancos de Wall Street) fueron las que más sufrieron. Por lo tanto, las empresas deben comprender y promover que los diferentes individuos y grupos dentro de la organización definen el riesgo del que son responsables, los posibles sesgos en las evaluaciones de riesgos y los desafíos en la implementación de iniciativas de gestión de riesgos (Bromiley et al., 2015).

Hasta hace poco, los riesgos financieros (como los de crédito y de mercado) y los riesgos de reputación eran los más preocupantes para los líderes de las organizaciones empresariales. Sin embargo, los riesgos operativos están ganando importancia, particularmente debido al desarrollo de la tecnología de la información (Doo, 2019).

Kalia y Müller (Kalia, Müller, 2015) explican en su libro que la idea de “Operational Risk Management” apareció por primera vez en la década de 1990 y que, por lo tanto, el campo se expandió para incluir el riesgo operativo. La Figura 1 muestra cómo ha evolucionado el enfoque de gestión de riesgos en las empresas a lo largo del tiempo, y

en particular, el riesgo operacional, desde su aparición en los documentos de Basilea II en la década de 1990.

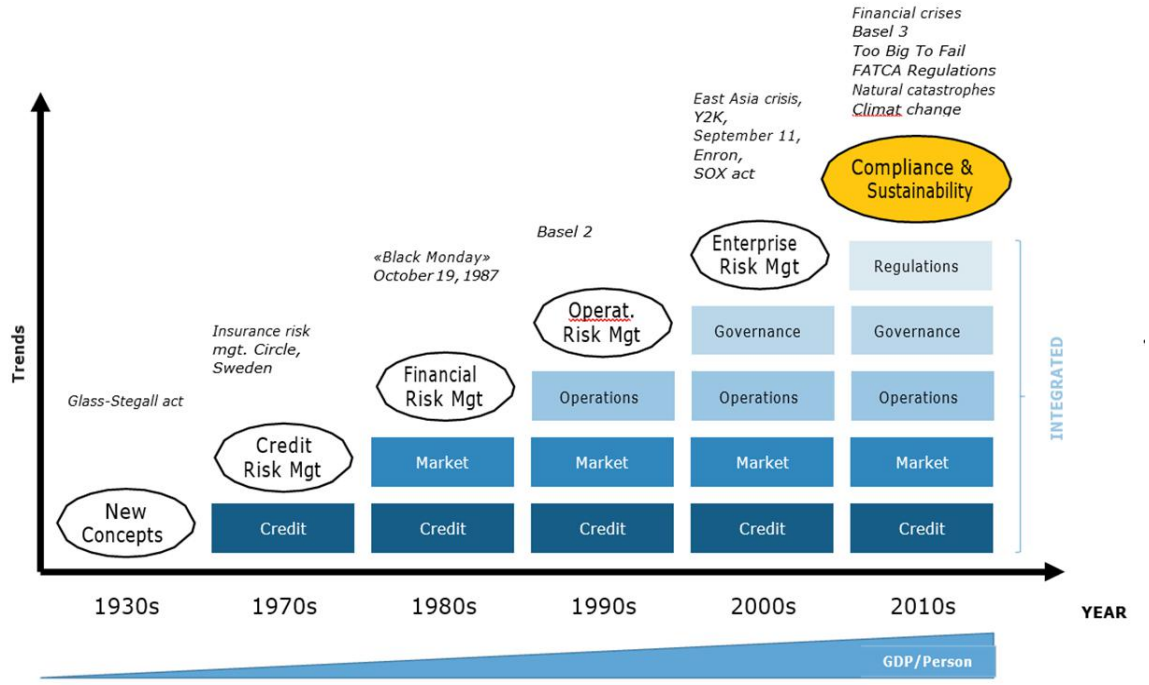


Fig. 1 Evolución de la Gestión de Riesgos. Fuente Kalia y Müller (2015, p. 59).

El riesgo operacional se define como el riesgo de pérdida directa o indirecta que resulta de procesos internos inadecuados o fallidos (Basilea II-BCBS 2001), personas y sistemas, o de eventos externos. Karam y Planchet (Karam, Planchet, 2012) demostraron que la importancia de los riesgos operativos ha aumentado hasta el punto en que ya no se consideran riesgos menores; son un factor importante en la posibilidad de consecuencias fatales para las empresas (especialmente en el sector financiero). Los siete riesgos operativos identificados en Basilea II son: fraude interno; fraude externo; prácticas

laborales y seguridad laboral; clientes, productos y prácticas comerciales; daño a activos físicos; interrupción del negocio; fallas del sistema y gestión de ejecución, entrega y proceso.

La seguridad se define en la Guía ESRM (ASIS International, 2019) como la condición de estar protegido contra peligros, amenazas, riesgos o pérdidas. Tras una revisión de la literatura académica y con el propósito de investigar la demarcación conceptual y científica de seguridad corporativa (security) frente a otras seguridades como la laboral (safety) industrial, etc; Jore (Jore, 2019) propone definir "security" como la capacidad percibida o real de prepararse, adaptarse, resistir y recuperarse de los peligros. y crisis causadas por actos deliberados, intencionales y maliciosos de las personas, como terrorismo, sabotaje, crimen organizado o piratería. Entre los siete riesgos operativos identificados en Basilea II, podemos ver que, ya sea de manera directa o transversal, la seguridad debería participar activamente en la gestión de algunos de esos riesgos operativos.

3.

MARCO TEÓRICO.

3.3.

Enterprise Security Risk Management (ESRM)

La gestión de riesgos de seguridad empresarial se define como un enfoque estratégico de la gestión de la seguridad que vincula la práctica de seguridad de una organización con su misión y objetivos, utilizando principios de gestión de riesgos establecidos y aceptados a nivel mundial; y donde el riesgo de seguridad se considera como el potencial de que una amenaza dada explote las vulnerabilidades para causar daño, pérdida o daño a un activo (ASIS International, 2019). En cuanto a la gestión del riesgo de seguridad, Jore (Jore, 2019) considera que la misma incluye evaluar y reducir la probabilidad y consecuencias de posibles ataques implementando diversos tipos de medidas de reducción del riesgo, como por ejemplo estableciendo protección de infraestructuras críticas y fortaleciendo la resiliencia organizacional.

Arena et al. (Arena, M. et al., 2014) proponen un modelo conceptual para la investigación en sistemas ERM a partir de la literatura de gestión estratégica, y también enfatizan que la mayoría de los trabajos que muestran modelos y enfoques para implementar ERM han sido desarrollados por profesionales o asociaciones profesionales.

ASIS International, la asociación profesional más importante de gerentes y profesionales de seguridad en todo el mundo, ha jugado un papel importante en las últimas décadas en la mejora de un nuevo paradigma de seguridad en el contexto de la gestión de riesgos; así, allanando el camino para la progresión desde una convergencia física y cibernética de la seguridad (Tyson, 2007) hacia un modelo holístico vinculado a ERM (Johnson, Spivey, 2008). La primera gran iniciativa fue la creación conjunta ASIS-ISACA de la Alianza para la Gestión de Riesgos de Seguridad Empresarial (AESRM) en 2005, donde se propuso que la ESRM requiere una colaboración multifuncional en el contexto de ERM entre varias áreas de gestión, incluidas, seguridad física y lógica, prevención de riesgos laborales, legal, gestión de riesgos, gestión de crisis y planificación de la continuidad del negocio.

ASIS International ha continuado trabajando en el desarrollo de ESRM con ese enfoque holístico, que se reflejó en su documento 'Enterprise Security Risk Management: A Holistic Approach to Security' (CSO Roundtable, 2015). Más adelante, Petruzzi y Loyear (Petruzzi, Loyear, 2016b) exploran los conceptos básicos de la filosofía y el ciclo de vida de ESRM. Dicha filosofía anima a todos los sectores de la empresa a reconocer y afrontar de forma proactiva el riesgo desde la perspectiva de la seguridad, presentando un modelo que contribuye sustancialmente a la resiliencia organizacional a lo largo del ciclo representado en la Fig.2.

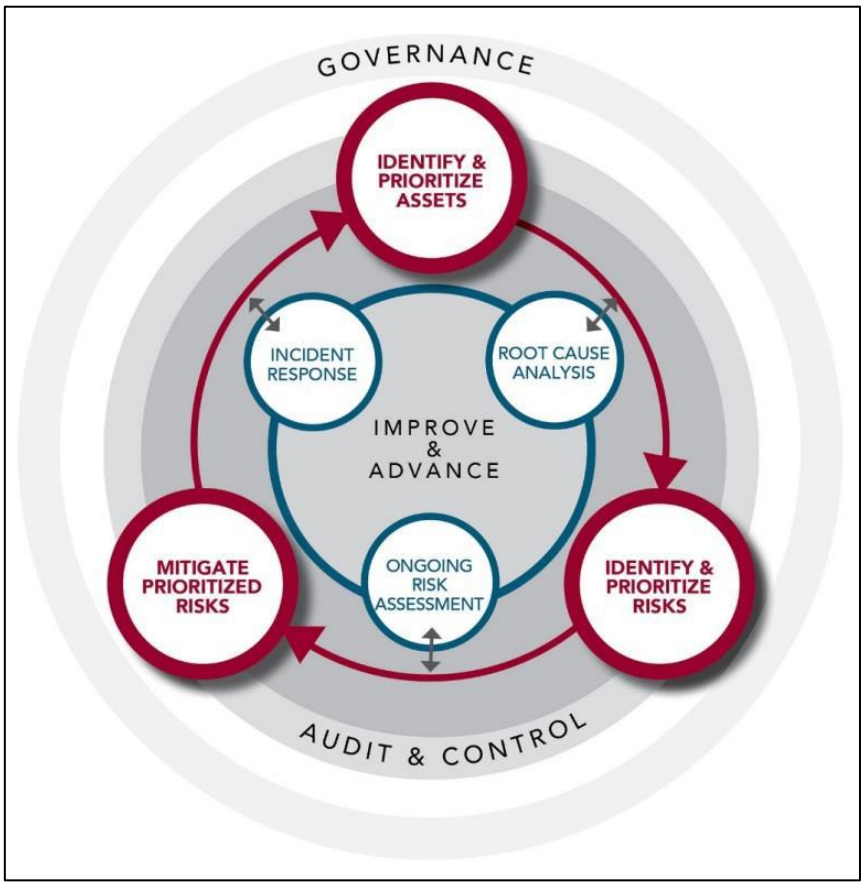


Fig. 2 Ciclo de gestión de riesgos de seguridad empresarial. Fuente Allen, B. Consultado el 15 de marzo de 2020.

ESRM se define como la aplicación de los principios fundamentales de riesgos para gestionar todos los riesgos de seguridad, ya sean relacionados con la información, cibernética, seguridad física, gestión de activos o continuidad del negocio, en un enfoque integral, holístico y global (Allen, B. J., Loyear, R., 2017).

Allen et al. (Allen et al., 2018) analizaron algunos casos de estudio en empresas sobre la implementación ERM de gobierno corporativo y gestión de riesgos y describieron cómo los principios fundamentales de gestión de riesgos basados en la filosofía de gobierno

corporativo y ERM pueden ser utilizados por los gestores de negocio en una organización para gestionar los riesgos de security. Proponen que la clave para administrar el riesgo de security en un modelo de gobierno es comprender que el riesgo de security es simplemente un subconjunto más de todos los riesgos que deben administrarse de manera integral en toda la empresa. Aunque el riesgo de security puede requerir acciones de mitigación y respuesta de riesgo altamente especializadas, el proceso de gestión de riesgos con principios fundamentales de riesgo es el mismo para el riesgo de seguridad, financiero, operativo o de otro tipo. En el gobierno corporativo el órgano de control a cargo de todo el ERM es el consejo de administración, y posteriormente en el ESRM debe ser también un modelo de gobierno para los riesgos de seguridad. Después de analizar esos estudios de caso, se encontraron tres modelos básicos que se pueden utilizar como marco para organizar la gobernanza de riesgos de seguridad en casi cualquier empresa: comité de security (con o sin subcomités), comités por dominios de seguridad, o redes de seguridad / grupos de trabajo.

ASIS ESRM Guideline es la visión actual de ESRM, y la primera herramienta de gestión de seguridad estratégica de su tipo, elevando la función de seguridad al establecer una asociación entre los profesionales de la seguridad y los líderes empresariales para gestionar los riesgos de seguridad (ASIS International, 2019). De acuerdo con esta guía, la gobernanza de la ESRM la lleva a cabo el órgano de control de seguridad de la organización (ej: un comité, consejo o grupo de gobernanza).

3.

MARCO TEÓRICO.

3.4.

Sistemas de Gestión

Las organizaciones precisan de normas reconocidas a nivel nacional o internacional que faciliten el diseño e implementación de un sistema de gestión en un área concreta, desarrollándose en un principio a partir de normas sobre la calidad, el medio ambiente y la seguridad y salud en el trabajo. Estas normas les permiten dotarse de una estructura y fundamentación clara para acometer dicha gestión. las normas principalmente aplicadas son la norma ISO 9001 en gestión de calidad, la norma ISO 14001en gestión ambiental e ISO 45001 para la gestión de la seguridad y salud en el trabajo.

La mayor parte de los sistemas de gestión basados en el estándar ISO tienen la siguiente estructura o están siendo migrados a dicho modelo:

- Objeto y campo de aplicación.
- Normas para consulta.
- Términos y definiciones.
- Contexto de la organización.
- Liderazgo.
- Planificación.
- Apoyo.

- Operación.
- Evaluación del rendimiento.
- Mejora.

El contenido de cada uno de los tres primeros apartados es específico de cada disciplina e incluso cada estándar puede tener su propia bibliografía asociada. Desde el punto de vista de gobierno y cumplimiento, los restantes siete apartados podrían ser perfectamente medibles en cualquier organización que pretenda implementarlo y podría por tanto determinarse un objetivo deseable de nivel de madurez.

3.

MARCO TEÓRICO.
3.5.

Modelos de Sistemas de Gestión de Seguridad

Resumen de normas relacionadas con Security

- ISO 31000
- ISO 28000
- ISO 27001
- ESRM Guideline (ASIS)
- ANSI/ASIS/RIMS RA1-2015
- ANSI/ASIS PAP.1: 2012
- ANSI/ASIS PSC.1: 2012

3.

MARCO TEÓRICO.
3.6.

Sistemas integrados de Gestión

Por razones de eficacia en su implementación, disminución de burocracia, facilidad en su auditabilidad, y una mejor visión unitaria, las organizaciones tienden a desarrollar sistemas integrados de gestión de tal manera que, en vez de mantener cada sistema de gestión separados en silos, sus componentes están vinculados (Calvo, Zapata, 2010), independientemente de qué función dentro de la compañía sea finalmente responsable de gobernarlos dentro de su área de responsabilidad. Otros autores destacan que con esta integración se utilizan recursos comunes en apoyo de la mejora de la satisfacción de los grupos de interés (Bernardo et al., 2017). La Organización Internacional de Normalización (ISO), también ha contribuido a la integración de estos sistemas de gestión, especialmente debido a las analogías y la compatibilidad de dichas normas. como ISO 9001, ISO 14001 e ISO 45001.

Según la Asociación Española para la Calidad, *para diseñar un sistema integrado de gestión, debemos partir de la gestión por procesos***.** Existen varios estándares para la integración de los sistemas

- *UNE 66177 de sistemas de gestión: una guía para la integración de los sistemas de gestión*. Incluye tres métodos denominados respectivamente método básico, método avanzado y método experto, aplicándose uno u otro en función de la madurez o experiencia que tenga la empresa en la gestión por procesos. Esta norma establece que la integración depende del nivel de madurez en la gestión por procesos, considera la gestión por procesos como mejor método para la integración de los sistemas de gestión.

- *PAS 99: una especificación de requisitos para sistemas integrados de gestión,* elaborada por The British Standards Institution (BSI). Aplicable para aquellas organizaciones que tienen basado su sistema de gestión en dos o más normas, como ISO 9001, ISO 14001, OHSAS 18001 u otras.

- El *Anexo SL*, cuya versión inicial fue la Guía ISO 83, introdujo facilidad de interpretación de cara a integrar varios sistemas de gestión.

3.

MARCO TEÓRICO.

3.7.

Justificación del Modelo propuesto

El investigador principal ha realizado estudios previos sobre modelos de gobernanza para riesgos de seguridad basados en ESRM, observando una brecha en el ámbito académico y técnico/profesional de un modelo específico en el que determinar la madurez de un sistema de gestión de la security vinculado con la gobernanza organizacional y ERM a través de un programa de ESRM.

ESRM es un marco que requerirá su implementación a través de acciones tangibles, teniendo en cuenta la especificidad de cada organización. Por este motivo se ha desarrollado el modelo de madurez del sistema de gestión de security, denominado ERMsec ©, alineado con la Guía ESRM de ASIS International y otros estándares internacionales, que debería ser flexible para cualquier tipo de organización y compatible con su sistema integrado de gestión de riesgos.

3.

MARCO TEÓRICO.
3.8.

Estructura del Modelo ERMsec ©

a) Nivel de Madurez

- 0 Inexistente / No deseado. - No existen políticas documentadas, no hay prestación del servicio o del proceso, no hay estructura organizativa ni recursos establecidos o no se dispone de métricas.

- 1 Inicial. - Es característico de los procesos en este nivel que están (típicamente) indocumentados y en un estado de cambio dinámico, que tiende a ser impulsado de manera ad hoc, incontrolada y reactiva por los usuarios o a causa de eventos. Esto proporciona un entorno caótico o inestable para los procesos.

- 2 Repetible. - Es característico de los procesos en este nivel que algunos procesos sean repetibles, posiblemente con resultados consistentes. Es poco probable que la disciplina del proceso sea rigurosa, pero donde existe, puede ayudar a garantizar que los procesos existentes se mantengan en momentos de estrés.

- 3 Definido. - Es característico de los procesos en este nivel que haya procesos estándar definidos y documentados establecidos y sujetos a cierto grado de mejora a lo largo del tiempo. Estos procesos estándar están implementados (es decir, son los procesos AS-IS) y se utilizan para establecer la consistencia del rendimiento del proceso en toda la organización.

- 4 Gestionado y medible. - Es característico de los procesos en este nivel que, al usar métricas de proceso, la Dirección puede controlar efectivamente el proceso AS-IS (por ejemplo, para el desarrollo de software). En particular, la Dirección puede identificar formas de ajustar y adaptar el proceso a proyectos particulares sin pérdidas medibles de calidad o desviaciones de las especificaciones. La Capacidad del Proceso se establece a partir de este nivel.

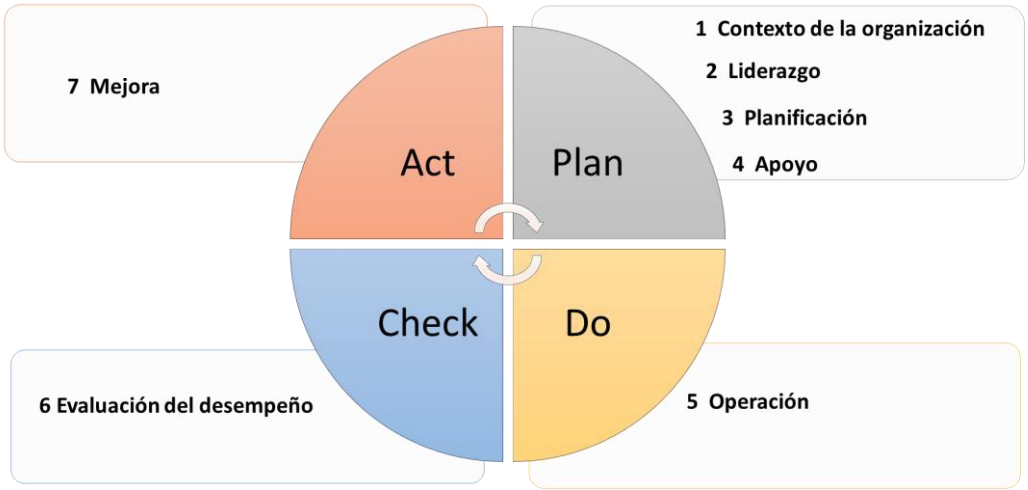
- 5 Optimizado. - Es una característica de los procesos en este nivel que el enfoque se centre en el rendimiento del proceso de mejora continua a través de cambios tecnológicos innovadores y progresivos.

b) Equivalencia de normas

Las normas y estándares internacionales objeto de correlación han sido, entre otros:

- COSO ERM - 2017
- ESRM (Maturity Assessment)
- UNE-EN-ISO 22301:2019
- ISO 22316:2017
- UNE-ISO 28000:2007
- UNE-ISO 31000:2018
- UNE 166006:2018
- UNE-EN ISO/IEC 27001
- ANSI/ASIS/RIMS RA1-2015
- ANSI/ASIS PAP.1: 2012
- BS 65000:2014

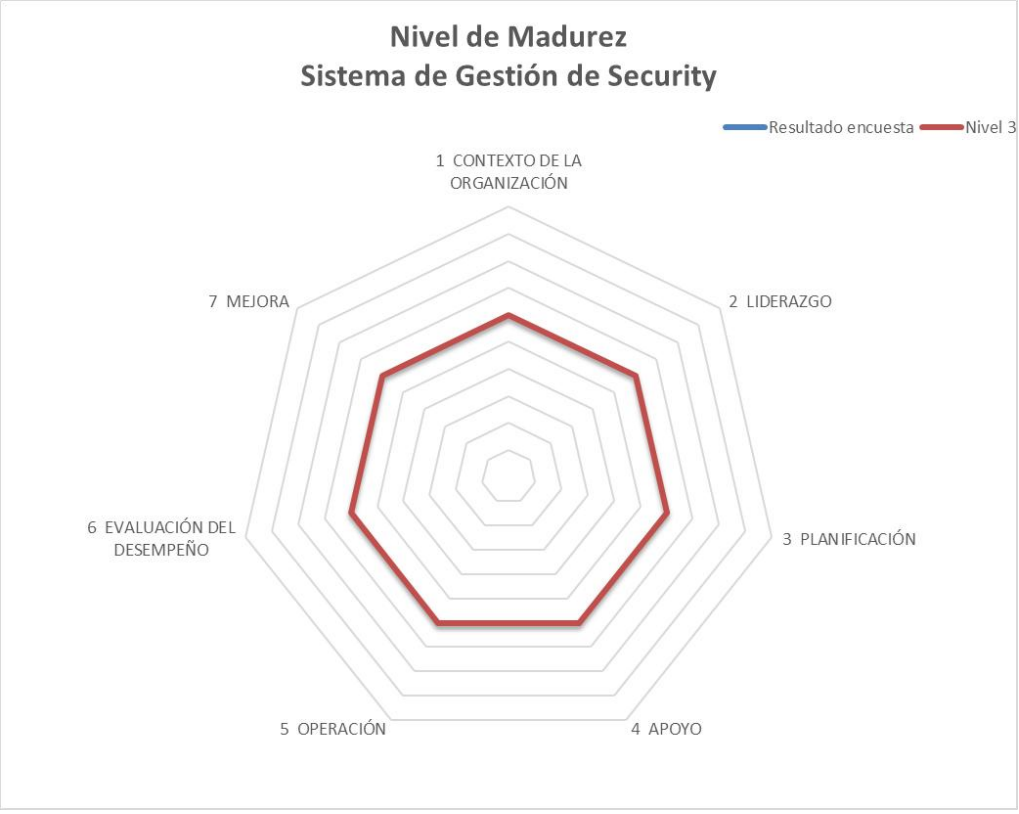
c) Estructura de sistemas de gestión basados en ISO y relación con ciclo de Deming.



P D C A	ESTRUCTURA
PLAN	1 CONTEXTO DE LA ORGANIZACIÓN
	2 LIDERAZGO
	3 PLANIFICACIÓN
	4 APOYO
DO	5 OPERACIÓN
CHECK	6 EVALUACIÓN DEL DESEMPEÑO
ACT	7 MEJORA

d) Gráfico radial con el grado (0 a 5) obtenido del cuestionario en relación con el objetivo.

Para este estudio se ha establecido como objetivo de referencia el nivel de madurez 3 (definido), puesto que podría ser considerado como un nivel óptimo para cualquier organización (destacado en color rojo en el gráfico).



4.

METODOLOGÍA

Tras una revisión de literatura académica sobre metodología de investigación, a través de consulta en la reconocida base de datos académica Web of Science (WoS) de Clarivate Analytics, se ha observado que algunos autores han estudiado la metodología de investigación académica / científica en contrapartida a otras metodologías utilizadas por investigadores en gestión operacional más interesados en resolver problemas relevantes y específicos (Will M. Bertrand, Fransoo, 2002). En este proyecto se han tomado como referencia estudios académicos sobre la metodología de la investigación cuantitativa (Casas Anguita, Repullo Labrador & Donado Campos, 2003) (López-Roldán, Fachelli, 2015). Finalmente se ha establecido ocho etapas en la planificación de la investigación utilizando la técnica de encuesta (Santesmases Mestre, 2009). La última etapa de "análisis de datos e interpretación de los resultados" se verá desarrollada a posteriori en sendos apartados de "resultados" y "discusión".

1. Identificación del problema.
2. Determinación del diseño de investigación.
3. Especificación de las hipótesis.
4. Definición de las variables.
5. Selección de la muestra.
6. Diseño del cuestionario.
7. Organización del trabajo de campo.
8. Obtención y tratamiento de los datos.
9. Análisis de los datos e interpretación de los resultados.

4.

METODOLOGÍA.

4.1.

Identificación del problema

La actividad empresarial está sometida a riesgos dentro de un entorno de incertidumbre. Parte de esos riesgos están relacionados con security. La gestión de estos debe estar integrada con la estrategia global de riesgos de organización, junto con el resto de las áreas corporativas y de negocio; y cobra cada vez más importancia, fundamentalmente, en las grandes organizaciones. De ahí que el planteamiento principal de este estudio sea analizar, basándose en estándares reconocidos internacionalmente (entre otros ESRM e ISO 31000), la gestión de riesgos de security en las empresas; principalmente las incluidas en el índice principal de referencia de la bolsa española (Ibex 35), y diagnosticar su contribución estratégica a la resiliencia de su organización.

Objetivos generales:

- Explorar el modelo de organización de Security en las principales empresas de España
- Evaluar el nivel de madurez del sistema de gestión de Security con respecto a estándares reconocidos internacionalmente, con un modelo que permita visualizar su evolución en próximos estudios. Para ello se utilizará el modelo ERMsec ©

Objetivos Secundarios

- Incorporar en el resultado de la encuesta las posibles necesidades de formación de seguridad de las empresas.
- Obtener resultados que permitan explorar futuras líneas de investigación.
- Comparar los sistemas de gestión de security en diferentes sectores.

4.

METODOLOGÍA.

4.2.

Determinación del diseño de investigación

La técnica de investigación seleccionada para esta investigación es la encuesta de carácter cuantitativo. Tomando como referencia la clasificación de Sierra (Sierra Bravo, 2007) el tipo de encuesta seleccionado viene cualificado por otros aspectos:

Finalidad: aplicada

Alcance: seccional

Profundidad: descriptiva

Amplitud: microsociológica

Fuentes: primarias

Naturaleza: no experimental.

4.

METODOLOGÍA.
4.3.

Especificación de las hipótesis

- Las principales empresas que cotizan en la bolsa de Madrid gestionan los riesgos de security a través de un sistema de gestión liderado por un Departamento de Seguridad formalmente constituido.

- La madurez del sistema de gestión de security está condicionada al apoyo de la alta dirección, reflejado en una política de security.

- La estrategia de seguridad está alineada con los objetivos de la organización y en ella se basan los objetivos y planificación para alcanzarlos.

- Al frente de los departamentos de seguridad corporativos existe un responsable con habilitación administrativa de Director de Seguridad asociada a la formación establecida por el regulador, que por el contrario no es exigible al resto de su equipo en el departamento.

4.

METODOLOGÍA.

4.4.

Definición de las variables

Variables simples

- Explorar el modelo de organización de Security en las principales empresas de España
- Evaluar el nivel de madurez del sistema de gestión de Security con respecto a estándares reconocidos internacionalmente, con un modelo que permita visualizar su evolución en próximos estudios. Para ello se utilizará el modelo ERMsec ©

Variables secundarias

- Incorporar en el resultado de la encuesta las posibles necesidades de formación de seguridad de las empresas.
- Obtener resultados que permitan profundizar sobre el estado del arte del proceso de Inteligencia.
- Comparar los sistemas de gestión de security en diferentes sectores.

Los indicadores de las variables implicadas en el objetivo de la encuesta serán recogidas posteriormente en el cuestionario.

4.

METODOLOGÍA.
4.5.

Selección de la muestra

Como criterio de inclusión se ha determinado que las empresas a entrevistar han de estar incluidas en el índice de la bolsa de Madrid, preferiblemente en el IBEX 35, lo que va a reducir el tamaño de la muestra. El listado se extrajo de la página web de la bolsa de Madrid, incluyendo los sectores a los que pertenece cada una.

4.

METODOLOGÍA.
4.6.

Diseño del cuestionario

Las instrucciones y formulación de preguntas son iguales para todos los sujetos y la información se recopila en un cuestionario, de tal forma que permite hacer comparaciones entre los diferentes subgrupos del estudio (sectores de actividad).

Preguntas de encuesta

El cuestionario inicial fue sometido a una prueba piloto con una de las empresas seleccionadas para el estudio, tras lo cual se realizaron las oportunas correcciones. Para reducir el cuestionario a 40 preguntas y mantener las secciones originales, se hizo un esfuerzo en identificar los indicadores clave de cumplimiento transversal de las normas internacionales en las que se basa el sistema de gestión propuesto, sobre todo en la sección que contenía las valoraciones del sistema de gestión. El número de indicadores clave puede variar entre 3 y 5 por cada pregunta de encuesta. Para ayudar a la cuantificación en la valoración del nivel de madurez (de 0 a 5) se determinó la siguiente escala de referencia:

1 - Inicial: Se cumple alguno de los requerimientos.

5- Optimizado: Se cumplen todos los requerimientos.

Organización de preguntas.

Las preguntas se organizan en 2 secciones:

- Datos generales:
  - ¿Su compañía pertenece al IBEX?
  - ¿A qué sector pertenece?
  - ¿Existe Departamento de Seguridad habilitado por el Ministerio de Interior?
  - ¿Cuántos niveles jerárquicos hay entre el Director de Seguridad y el CEO?
  - ¿A qué Dirección/Función reporta el Departamento de Seguridad?
  - ¿Cuántos empleados (no contratas) están encuadrados en el Departamento de Seguridad?

- Datos específicos del sistema de gestión:
    1. Contexto de la organización.
    2. Liderazgo.
    3. Planificación.
    4. Apoyo.
    5. Operación.
    6. Evaluación del desempeño.
    7. Mejora.

4.

METODOLOGÍA.

4.7.

Organización del trabajo de campo

Se ha estimado adecuado que la encuesta sea a través de entrevista personal para asegurar un alto grado de respuesta (León, Montero, 1993) y que, al haber un contacto directo, se puede hacer aclaraciones de forma instantánea; pudiendo ser un factor limitante la extensión del cuestionario por el tiempo a dedicar por entrevistador y entrevistado. Se exige además un marco de confianza mutuo para garantizar el anonimato, que puede requerir de previo acuerdo formal o informal. Al estar incluido el cuestionario en una herramienta previamente desarrollada por el investigador, permite disponer del resultado inmediatamente y facilitar una copia anonimizada al entrevistado.

4.

METODOLOGÍA.
4.8.

Obtención y tratamiento de los datos

Los datos son codificados atendiendo a las valoraciones objetivas y las secciones del cuestionario, pasando a formar parte de una base informatizada para posterior tratamiento estadístico. Del tratamiento de esos datos en MsExcel se han extraído gráficos, tanto en forma clásico como los que proporciona la propia herramienta a través de los llamados “key influencers” de Power BI. En estos últimos, los datos no reflejan valores absolutos pero que permiten identificar relaciones y patrones entre las diferentes secciones de la encuesta que faciliten su interpretación.

5.

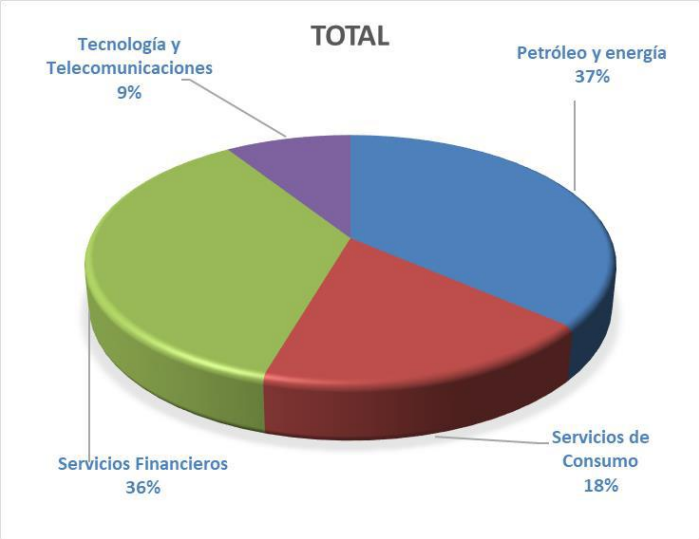
RESULTADOS DEL ANÁLISIS.

5.1.

Datos Generales

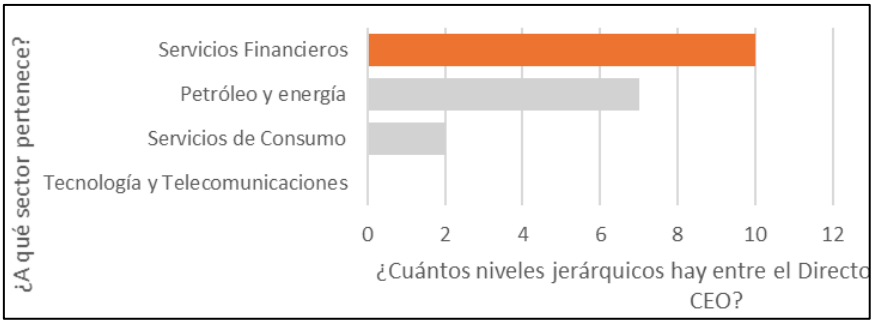
- Todas las empresas encuestadas disponen de departamento de seguridad debidamente formalizado conforme a la Ley de Seguridad Privada.
- El 73% de las empresas encuestadas pertenecen al IBEX 35

- Están encuadradas en 4 de los 7 sectores en los que se dividen las empresas cotizadas en bolsa.



- Sólo un 18% reporta directamente al CEO, el 9% reporta a un miembro del comité de dirección, el 55% reporta a un directivo que no forma parte del comité de dirección y el 18% está en un cuarto nivel en la jerarquía de la compañía.

- El valor proporcional asociado a los niveles jerárquicos entre el Director de Seguridad y el CEO es notablemente superior en el sector de Servicios Financieros.



- La dirección/función a la que con más frecuencia reporta el Director de Seguridad es la de Recursos (46%), seguida de la misma proporción (18%) en su dependencia jerárquica directa del CEO, Operaciones o Personas.

5.

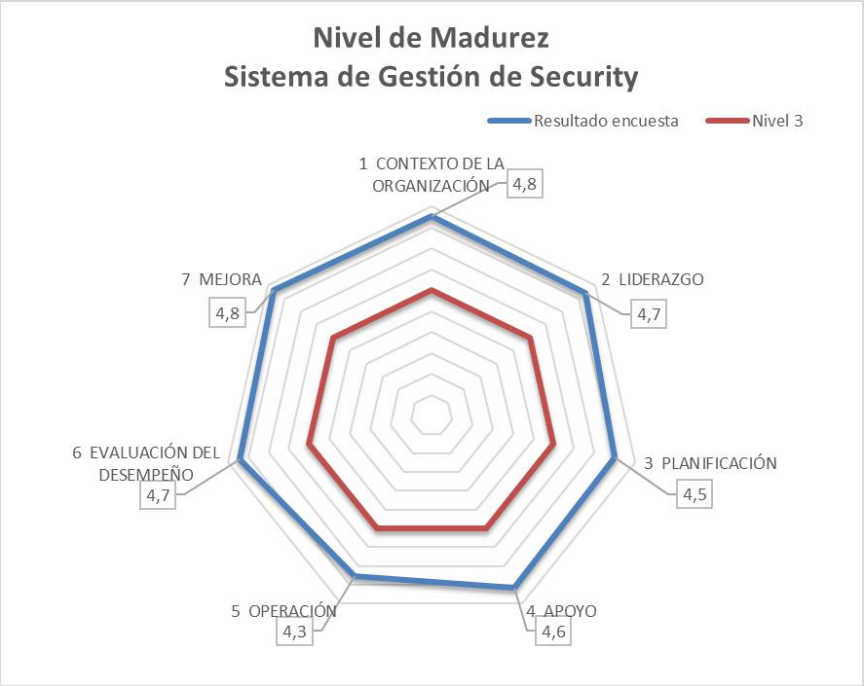
RESULTADOS DEL ANÁLISIS.
5.2.

Sistema de Gestión

- El resultado global en la escala CMMI (0-5) es de 4,6 de media ponderada, siendo el valor más bajo el de Operación (4,3) y el más alto (4,8) se da en Contexto de la Organización y en Mejora.

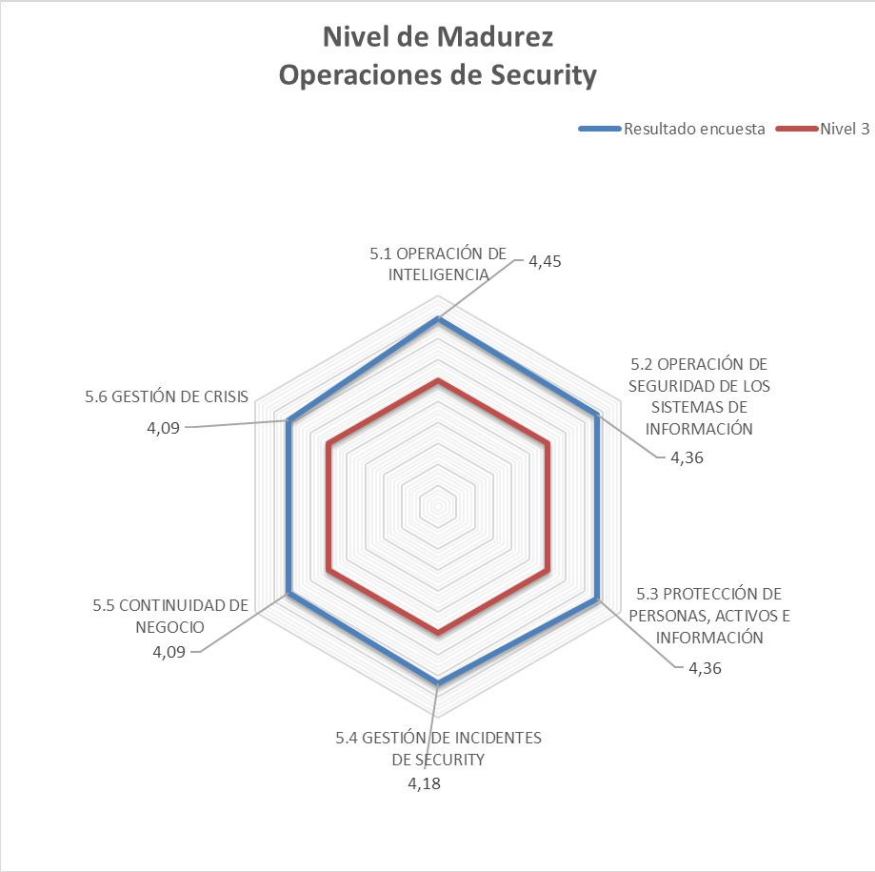
	NIVEL DE MADUREZ Sistema de Gestión de Security		
P D C A	ESTRUCTURA	Resultado encuesta	Nivel 3
PLAN	1 CONTEXTO DE LA ORGANIZACIÓN	4,8	3
	2 LIDERAZGO	4,7	3
	3 PLANIFICACIÓN	4,5	3
	4 APOYO	4,7	3
DO	5 OPERACIÓN	4,3	3
CHECK	6 EVALUACIÓN DEL DESEMPEÑO	4,7	3
ACT	7 MEJORA	4,8	3
		4,6	

- En el gráfico radial se ha marcado en rojo el nivel 3, que se correspondería al nivel de madurez “Definido”. En azul se representa los valores alcanzados y que entrarían en el tramo más alto del nivel 4, correspondiente al grado de madurez “Gestionado y medible”.



- En el apartado de Operaciones el resultado es de 4,26 de media ponderada, siendo el valor más bajo el correspondiente a las operaciones de Continuidad de Negocio y Gestión de Crisis (4,09) y el más alto (4,45) se da en la operación de Inteligencia. Tanto el valor mínimo como el máximo están en el grado de madurez 4, correspondiente al nivel de madurez "Gestionado y medible".

	5 OPERACIÓN	Resultado encuesta
DO	5.1 OPERACIÓN DE INTELIGENCIA	4,45
	5.2 OPERACIÓN DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN	4,36
	5.3 PROTECCIÓN DE PERSONAS, ACTIVOS E INFORMACIÓN	4,36
	5.4 GESTIÓN DE INCIDENTES DE SECURITY	4,18
	5.5 CONTINUIDAD DE NEGOCIO	4,09
	5.6 GESTIÓN DE CRISIS	4,09
		4,26



- Se ha evaluado si la alta dirección demuestra liderazgo y compromiso con el sistema de gestión de security a través de los siguientes parámetros:

1. Asegurarse de que se establezcan las políticas y los objetivos del sistema de gestión, y que estos sean compatibles con la dirección estratégica de la organización.

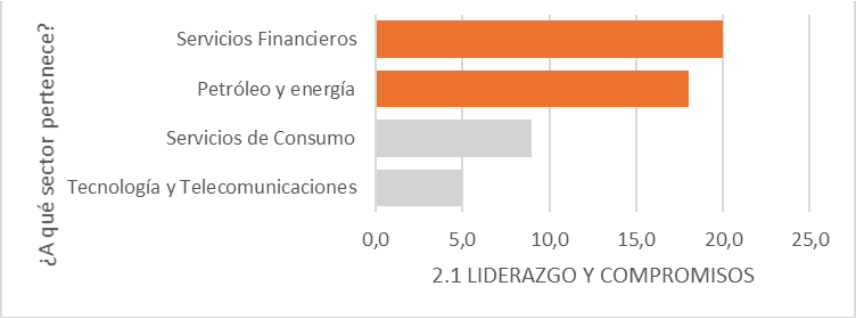
2. Asegurarse de la integración de los requisitos del sistema de gestión en los procesos de negocio de la organización.

3. Asegurarse de que se dispone de todos los recursos necesarios para el Sistema de Gestión.

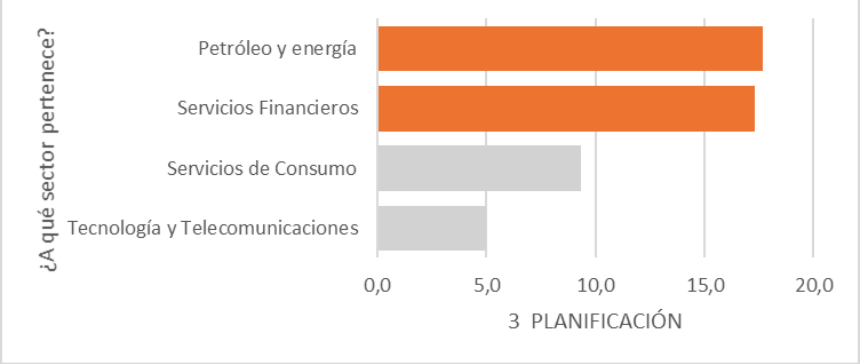
4. Se tiene que comunicar la importancia que tiene la gestión eficaz de Security conforme con los requisitos del Sistema de Gestión.

5. Se debe asegurar de que se consiguen todos los resultados previstos por la organización para el sistema de Gestión, y promover la mejora continua.

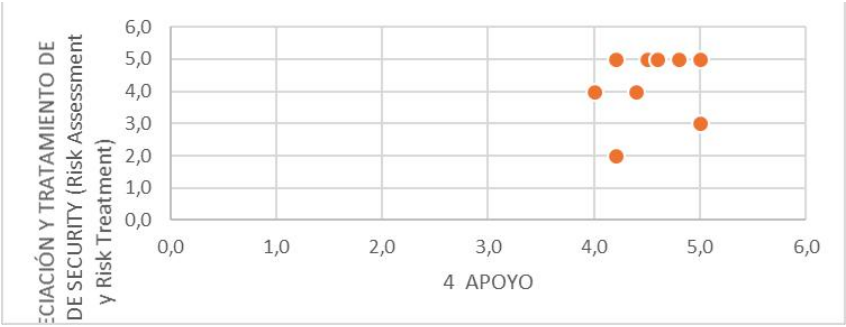
El valor proporcional asociado a LIDERAZGO Y COMPROMISO es ligeramente superior en el sector de Servicios Financieros, seguido del sector de Petróleo y Energía.



- El valor proporcional asociado a PLANIFICACIÓN es notablemente superior en el sector de Petróleo y Energía, seguido de Servicios Financieros.



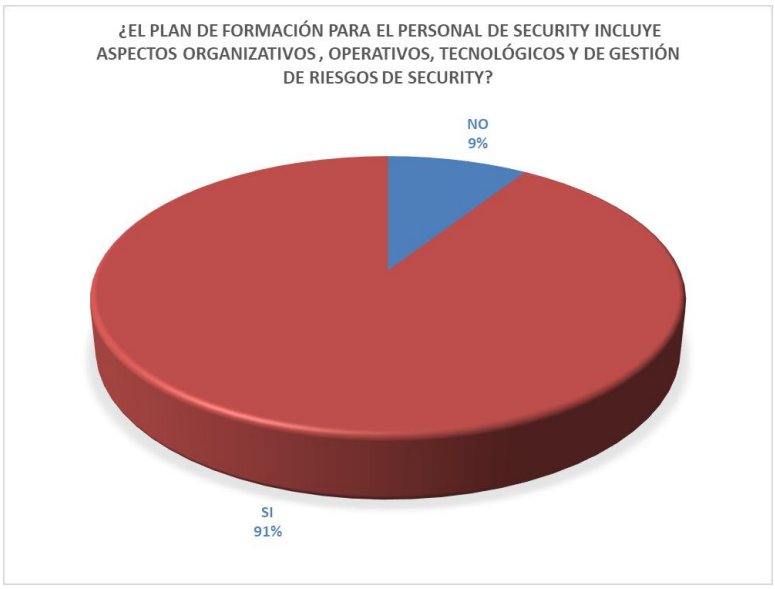
- Un valor alto en APOYO determina un valor alto en el proceso de APRECIACIÓN Y TRATAMIENTO DE RIESGOS



- El 82% de las empresas encuestadas tiene un plan de formación o concienciación específico de Security para todo el personal de la empresa. Un 9% lo tiene parcialmente implantado, y el 9% no dispone de ello.

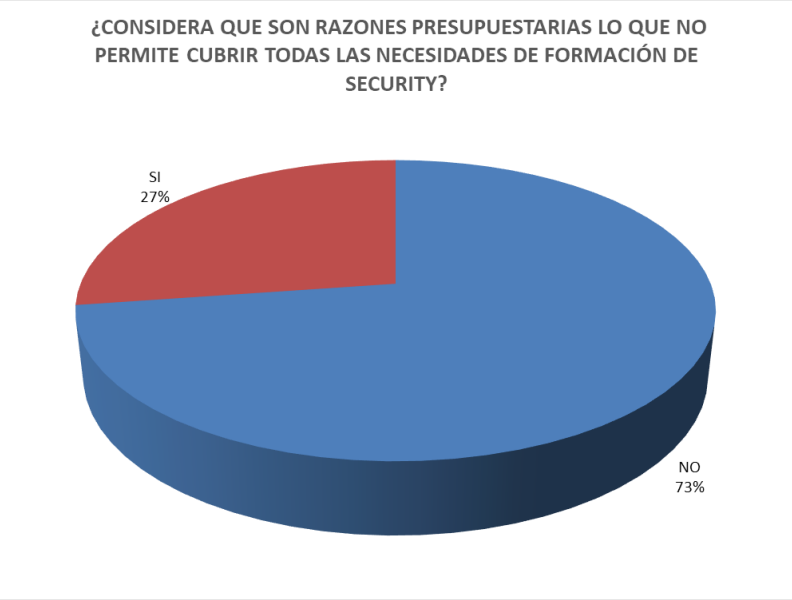
- El 82% de las empresas encuestadas tiene un plan de formación o concienciación específico de Security para el personal del Departamento de Seguridad. Un 9% lo tiene parcialmente implantado, y el 9% no dispone de ello

- En la mayoría de las empresas encuestadas (91%) el plan de formación para el personal del Departamento de Seguridad incluye aspectos organizativos, operativos, tecnológicos y de gestión de riesgos de security.



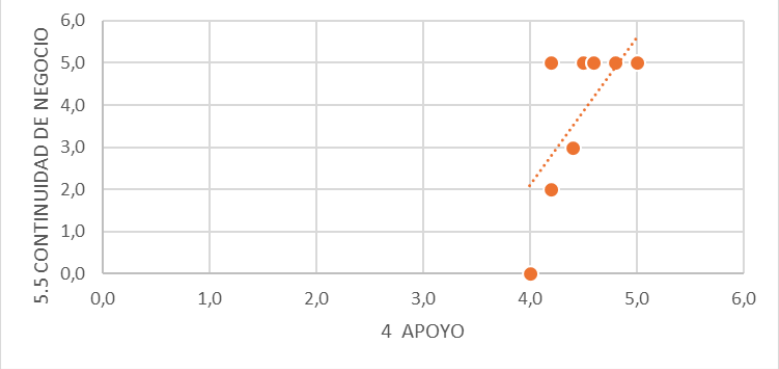
- El 64% considera que su organización no tiene cubiertas todas las necesidades de formación de security. Un 36% considera que sí.

- El 73% considera que el presupuesto es una de las razones que no permite cubrir todas las necesidades de formación de security.

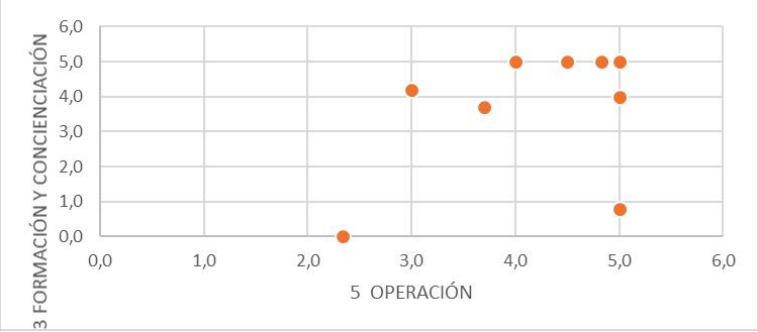


- La falta de formación en mercado es en un 73% de los casos otra razón que no permite cubrir las necesidades de formación de security.

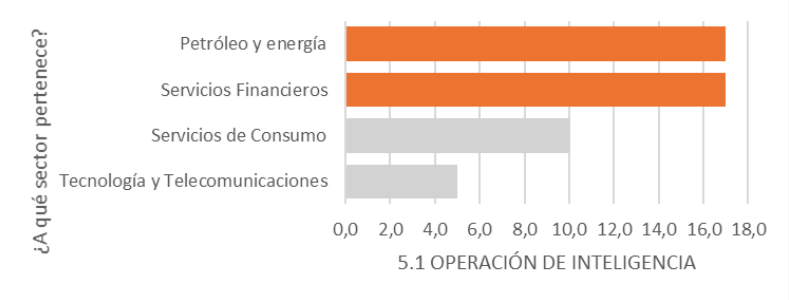
- Los valores de madurez en la operación de CONTINUIDAD DE NEGOCIO dependen proporcionalmente del APOYO.



- Un valor alto en OPERACIÓN determina generalmente un valor alto en FORMACIÓN Y CONCIENCIACIÓN

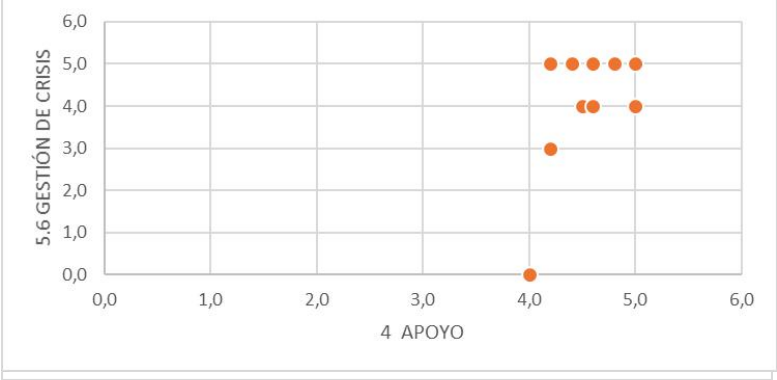


- El valor proporcional asociado a la OPERACIÓN DE INTELIGENCIA es notablemente superior en el sector de Petróleo y Energía, seguido de Servicios Financieros.

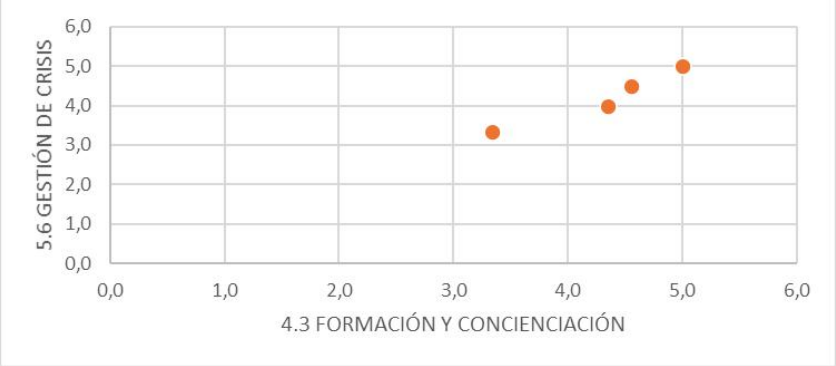


- El valor proporcional asociado a tener un programa de formación de security específico para el personal del Departamento de Seguridad es notablemente superior en el sector de Petróleo y Energía, seguido de Servicios Financieros.

- En general valores altos de APOYO dan lugar a valores altos en la operación de GESTIÓN DE CRISIS



- El campo FORMACIÓN Y CONCIENCIACIÓN y el de GESTIÓN DE CRISIS aparecen muy dependientes entre sí



6.

DISCUSIÓN

Todas las empresas encuestadas tienen un Departamento de Seguridad, pero ello no implica que en todas las empresas cotizadas exista departamento de seguridad constituido formalmente con un director de seguridad habilitado por el Ministerio de Interior.

Aunque un 18% de los Directores de Seguridad reportan directamente al CEO y un 9% a algún alto directivo en el comité de dirección, el departamento de seguridad se encuentra en gran medida encuadrado en un tercer o cuarto nivel jerárquico directo en la organización. La función a la que reporta en mayor medida el Director de Seguridad es a la Dirección de Recursos. Por otro lado, en la mayoría de las empresas encuestadas los Directores de Seguridad tienen un contacto directo con el presidente o el CEO de la compañía en tanto que gestionan directamente su seguridad (personal, protección, información sensible, etc.). El sector que está más cercano jerárquicamente al CEO es el de Tecnología y Telecomunicaciones, seguido de Servicios de Consumo, Petróleo y Energía, y Servicios Financieros.

Este estudio está muy enfocado a la gestión de la función de security y no es de extrañar que, aquellas empresas que han considerado la necesidad de constituir un área específica para gestionar los riesgos de seguridad hayan alcanzado un grado alto de madurez en los procesos de su sistema de gestión, quizás también porque la mayor parte de ellas llevan operando décadas y el proceso de mejora continua tiene un efecto palpable. Recordemos que, dentro de la estructura del sistema de gestión, el de Mejora tiene el grado de madurez más alto (4,8), el mismo grado que el resultado del de Contexto de la Organización. Es justo en ese punto entre la Mejora (Act) y el Contexto de la organización (Plan) donde se cierra (o empieza) el ciclo de Deming. En el gráfico radial del sistema de gestión de security se aprecia que los resultados mínimos y máximos están dentro del tramo más alto del nivel 4, que corresponde al grado de madurez "Gestionado y medible".

En los procesos de "Operación" del apartado quinto del sistema de gestión se han tenido en cuenta las operaciones más habituales desarrolladas en los departamentos de seguridad: Protección de Personas, Activos e Información y Gestión de Incidentes de Security. También se ha incorporado en este apartado de Operaciones otras disciplinas que han adquirido peso específico por el impacto de los riesgos asociados, como son: Inteligencia, Seguridad de los Sistemas de Información, Continuidad de Negocio y Gestión de Crisis. El valor más alto lo ha alcanzado la operación de Inteligencia, lo cual parece tener sentido por cuanto las organizaciones empresariales han de reducir la incertidumbre con respecto a los riesgos que puedan afectar a sus objetivos.

La inteligencia habitualmente ha estado más enfocada a la de "negocio" y subcontratada en muchas ocasiones en "expertos" en el mercado que tradicionalmente han conseguido un mejor posicionamiento de un producto o servicio. Sin embargo, ya no es suficiente con atender los riesgos financieros o de mercado, pues los operacionales (entre los que están las pandemias o los ciberataques a gran escala) ocupan ya los primeros puestos de preocupación de estados y grandes organizaciones empresariales, tal como se indica en el reciente informe del World Economic Forum. Las empresas multinacionales españolas, como muchas otras, se han visto obligadas a la búsqueda de "océanos azules" fuera de España, en aras de balancear la cuenta de resultados y de la diversificación de inversiones. Esta salida al exterior fuera de áreas tradicionales como Europa o América Latina ha enfrentado las estrategias de expansión a la realidad de un entorno de poca estabilidad económica e inestabilidad política y social. La mayor parte de las empresas encuestadas cuentan con personal muy especializado en inteligencia y capacitados para filtrar la ingente información del entorno, para después trasladar hacia la alta dirección sólo aquella que aporte valor en la toma de decisiones estratégicas de negocio.

En los valores más bajos del apartado Operación encontramos los correspondientes a las operaciones de Gestión de Incidentes (4,18), Continuidad de Negocio y de Gestión de Crisis (ambas con puntuación de 4,09). Las tres representan el "triángulo" de la resiliencia organizacional, aunque desde el departamento de seguridad tradicionalmente se ha visto más involucrado en la coordinación de la gestión de crisis, independientemente del escenario que provocó su activación.

Es habitual que la continuidad de negocio quede fuera del alcance de la responsabilidad exclusiva del departamento de seguridad, pues la unidad de negocio es la propietaria y gestora de sus riesgos, y que los frecuentes ciber incidentes enfoquen los planes de continuidad de negocio en su vertiente tecnológica y planes de recuperación de desastre. Se ha apreciado en las entrevistas una carencia en el liderazgo único de la resiliencia (gestión de crisis, continuidad de negocio y gestión de incidentes), plasmado en algunos casos en la ausencia de una política específica de resiliencia que aporte una línea de acción estratégica al frente de un único departamento, aunque por separado obtienen un alto grado de madurez. En cuanto a las operaciones de gestión de crisis y la de continuidad de negocio, se ha encontrado que valores altos en el apartado de Apoyo del sistema de gestión determinan un valor alto en ese proceso. También se ha visualizado que los valores del apartado de gestión de crisis son muy dependientes de los valores de formación y concienciación, lo que refuerza la idea de que una adecuada preparación de los miembros de los equipos de gestión de crisis influye sustancialmente en las capacidades operativas de preparación, respuesta y recuperación.

Se ha evaluado si la alta dirección demuestra liderazgo y compromiso con el sistema de gestión de security, asegurándose de que se establecen políticas compatibles con la estrategia de la compañía, la integración de los requisitos de este sistema de gestión en los procesos de negocio, dotándole de todos los recursos necesarios, comunicando su importancia, que se consiguen los resultados previstos, y promoviendo su mejora continua.

Es de destacar que para ellos es básico tener aprobada una política y que estén definidos los roles, responsabilidades y autoridad en la organización. Aunque los valores en general han sido muy altos en este apartado, es ligeramente superior en el sector de Servicios Financieros, seguido del sector de Petróleo y Energía.

En el apartado de Planificación se han tenido en cuenta las acciones para abordar riesgos y oportunidades de security, la apreciación y tratamiento de riesgos de security (risk assessment y risk treatment), así como los objetivos de security y la planificación para alcanzarlos. En los resultados se visualiza que este apartado es ligeramente superior en el sector de Petróleo y Energía, seguido del sector de Servicios Financieros. En cuanto a la apreciación y tratamiento de los riesgos, se ha encontrado que valores altos en el apartado de Apoyo del sistema de gestión determinan un valor alto en ese proceso asociado a los riesgos, lo cual hace suponer que, si se dispone de recursos con adecuada competencia y formación, además de una comunicación pertinente y un marco normativo/documental adecuado, ese proceso de apreciación y tratamiento del riesgo tendrá mejor consecución.

La formación ha tenido su propio apartado en este estudio, tanto en lo referido a formación/concienciación de todos los empleados como a la del personal del propio departamento de seguridad. Sólo un 18% de las empresas no tiene un programa específico para empleados o no lo tiene totalmente implantado.

Generalmente se imparte en el momento de la incorporación de cualquier empleado, dentro de su "paquete" de inducción, y periódicamente a través de campañas específicas a través de las redes de comunicación internas o campañas asociadas a un riesgo específico (ciberseguridad, fraude, etc.). Las mismas proporciones se han observado en la formación específica para el personal del departamento de security, siendo ligeramente superior en el sector de Petróleo y Energía, seguido del sector de Servicios Financieros. En la formación a personal del departamento de seguridad se incluyen aspectos organizativos, operativos, tecnológicos y de gestión de riesgos de security; aunque sin embargo el 64% considera que su organización no tiene cubiertas todas las necesidades de formación. Algunos de los encuestados han manifestado una carencia en formación específica para personal que no ocupa la posición de Director de Seguridad, concretamente en mandos intermedios y puestos técnicos. Por ejemplo: especialización en gestión e implementación de proyectos de seguridad, prevención de fraude, o investigación corporativa. Otros encuestados hacen referencia a formación relativa a inteligencia artificial y uso de Big Data, en relación con las operaciones de seguridad. Para encontrarla es preciso recurrir a formación en el extranjero o que haya adquirido esa experiencia previamente en otras organizaciones públicas o privadas. El 73% considera que la insuficiente oferta en el mercado es una razón por la que no se cubre todas las necesidades de formación de security, mientras que sólo el 23% lo achaca a razones presupuestarias. Por último, se evidencia en los resultados que un valor alto en formación y concienciación determina también un valor alto en el apartado de operaciones, lo cual parece lógico.

7.

CONCLUSIONES

Algunos autores advierten sobre la posibilidad de que la información obtenida no siempre refleje la realidad, pues se obtiene a través de una observación indirecta de los hechos, dependiendo de lo que los encuestados estén dispuestos a manifestar (Sierra Bravo, 2007). Por otro lado, un estudio más exhaustivo podría determinar cuál es la implementación real del sistema de gestión a través de indicadores clave de rendimiento en cada uno de los procesos de dicho sistema.

Otra de las limitaciones ha sido el no haber podido tener representados en la muestra a todos los sectores, cuestión que debería tenerse en cuenta en posteriores estudios, ampliando en lo posible el número e intentando tener un número proporcional que represente a cada sector.

Tras explorar el modelo de organización de Security en algunas de las más importantes empresas de España se ha determinado que en general existe un alto grado de madurez del sistema de gestión de Security, liderado por la figura del director de seguridad el cual no siempre reporta al primer nivel de la organización, aun contando con profesionales de reconocido prestigio.

Se aprecia una evolución en la tipología cada vez más amplia de operaciones que desarrolla el departamento de seguridad, aprovechando sus capacidades y experiencia como las áreas de inteligencia y gestión de crisis, aunque aún haya margen para su desarrollo.

La formación se ha mostrado un elemento clave en la implementación de la estrategia de seguridad. Sin embargo, existen carencias tanto en la oferta como en la creación de una cultura de seguridad embebida en todos los niveles de la organización; estando más avanzados aquellos sectores que, por requerimiento regulatorio o necesidades de expansión en áreas de alto riesgo, se han visto obligado a ello.

Derivado de este estudio se abren otras líneas de investigación en el plano estratégico para determinar la vinculación de la gobernanza organizacional y el cumplimiento (responsabilidad de los comités de dirección y consejos de administración) en la gestión de riesgos de seguridad y la resiliencia a través de un programa de ESRM (Marquez-Tejon, Jimenez-Partearroyo & Benito-Osorio, 2021). En estudios académicos recientes se ha observado que los modelos de gobernanza para riesgos de seguridad incluyen la constitución de comités o grupos de trabajo específicos (Allen et al., 2018), siendo factible realizar un estudio con ese enfoque entre las empresas españolas, ampliando la muestra también a “medianas” empresas. Por otro lado, el liderazgo que implica un programa ESRM y el éxito en obtener el apoyo de la alta dirección justificaría identificar y analizar las implicaciones gerenciales necesarias a futuro del responsable último de la seguridad en las organizaciones.

Desde el plano operativo, será interesante profundizar en otras áreas que han formado parte de este estudio como son las operaciones de inteligencia y resiliencia (gestión de incidentes, continuidad de negocio y gestión de Crisis).

8.

BIBLIOGRAFÍA

Allen, B. J., Loyear, R. 2017, *Enterprise Security Risk Management: Concepts and Applications,* Noakes-Fry, K. edn, .

Allen, B., Kelly, T., Loyear, R., Poole, A., Awojulu, A., Kmetetz, A., Rakotomavo, M., Wang, Z., Xu, H., Xu, M. & Yuan, H. 2018, "Security Risk Governance: A Critical Component to Managing Security Risk", *The journal of applied business and economics,* vol. 20, no. 1, pp. 132-146.

Arena, M., Azzone, G., Cagno, E., Silvestri, A. & Trucco, P. 2014, "A model for operationalizing ERM in project-based operations through dynamic capabilities", *International Journal of Energy Sector Management,* vol. 8, no. 2, pp. 178-197.

Arena, M., Arnaboldi, M. & Azzone, G. 2010, "The organizational dynamics of Enterprise Risk Management", *Accounting Organizations and Society,* vol. 35, no. 7, pp. 659-675.

Bennett, N. & Lemoine, G.J. 2014, "What a difference a word makes: Understanding threats to performance in a VUCA world", *Business horizons,* vol. 57, no. 3, pp. 311-317.

Bernardo, M., Gianni, M., Gotzamani, K. & Simon, A. 2017, "Is there a common pattern to integrate multiple management systems? A comparative analysis between organizations in Greece and Spain", *Journal of Cleaner Production,* vol. 151, pp. 121-133.

Bharathy, G.K. & McShane, M.K. 2014, "Applying a Systems Model to Enterprise Risk Management", *Engineering Management Journal,* vol. 26, no. 4, pp. 38-46.

Bromiley, P., McShane, M., Nair, A. & Rustambekov, E. 2015, "Enterprise Risk Management: Review, Critique, and Research Directions", *Long range planning,* vol. 48, no. 4, pp. 265-276.

Calvo, M.ÁC. & Zapata, M.ÁR. 2010, "Desarrollo de un modelo de sistema integrado de gestión mediante un enfoque basado en procesos", *4th International Conference on Industrial Engineering and Industrial Management*, pp. 1555.

Casas Anguita, J., Repullo Labrador, J.R. & Donado Campos, J. 2003, "La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (II)", *Atención primaria,* vol. 31, no. 9, pp. 592-600.

Crump, J. 2015, *Corporate security intelligence and strategic decision making,* Taylor and Francis.

Doo, S.I. 2019, "A Study on Legal Risk under Enterprise Risk Management & Management System Centered on the Board of Directors", *Journal of hongik law review,* vol. 20, no. 1, pp. 651-684.

Eastburn, R.W. & Sharland, A. 2017, "Risk management and managerial mindset", *The Journal of Risk Finance,* vol. 18, no. 1, pp. 21-47.

Gill, M. 2007, "The Challenges for the Security Sector: Thinking About Security Research", *Security Journal,* vol. 20, no. 1, pp. 27-29.

Govender, D. 2019, "The use of the risk management model ISO 31000 by private security companies in South Africa", *Security Journal,* vol. 32, no. 3, pp. 218-235.

Gupta, N. 2016, "Developing a Decision Support Enabled Enterprise Risk Control Framework for Sector Focused Indian Companies Transforming into Global Energy Enterprises", *Gurukul Business Review-Gbr,* vol. 12, pp. 46-53.

Hoyt, R. & Liebenberg, A. 2011, "THE VALUE OF ENTERPRISE RISK MANAGEMENT", *Journal of Risk and Insurance,* vol. 78, no. 4, pp. 795-822.

Johnson, M. & Spivey, J. 2008, "ERM AND THE SECURITY PROFESSION", *Risk Management,* vol. 55, no. 1, pp. 30-35.

Jore, S.H. 2019, "The Conceptual and Scientific Demarcation of Security in Contrast to Safety", *European Journal for Security Research,* vol. 4, no. 1, pp. 157-174.

Kalia, V. & Müller, R. 2015, *Risk Management at Board Level - A Practical Guide for Board Members,* 2nd edn, Haupt Bern, Austria.

Karam, E. & Planchet, F. 2012, "Operational risks in financial sectors", *Advances in Decision Sciences,* vol. 2012.

León, O.G. & Montero, I. 1993, *Diseño de investigaciones : introducción a la lógica de la investigación en psicología y educación,* McGraw-Hill, Madrid etc.

López-Roldán, P. & Fachelli, S. 2015, *Metodología de la investigación social cuantitativa,* Bellaterra: Universitat Autònoma de Barcelona, Bellaterra.

Ludbey, C.R., Brooks, D.J. & Coole, M.P. 2018, "Corporate Security: Identifying and Understanding the Levels of Security Work in an Organisation", *Asian Journal of Criminology,* vol. 13, no. 2, pp. 109-128.

Marquez-Tejon, J., Jimenez-Partearroyo, M. & Benito-Osorio, D. 2021, "Security as a key contributor to organisational resilience: a bibliometric analysis of enterprise security risk management", *Security Journal,* .

Martin, R. & Sunley, P. 2015, "On the notion of regional economic resilience: Conceptualization and explanation", *Journal of Economic Geography,* vol. 15, no. 1, pp. 1-42.

Mcshane, M., Nair, A. & Rustambekov, E. 2011, "Does Enterprise Risk Management Increase Firm Value?", *Journal of Accounting, Auditing & Finance,* vol. 26, no. 4, pp. 641.

Nalla, M. & Morash, M. 2002, "Assessing the Scope of Corporate Security: Common Practices and Relationships with Other Business Functions", *Security Journal,* vol. 15, no. 3, pp. 7-19.

Petruzzi, J. & Loyear, R. 2016a, "Improving organisational resilience through enterprise security risk management", *Journal of business continuity & emergency planning,* vol. 10, no. 1, pp. 44-56.

Petruzzi, J. & Loyear, R. 2016b, "Improving organisational resilience through enterprise security risk management", *Journal of business continuity & emergency planning,* vol. 10, no. 1, pp. 44-56.

Prewett, K. & Terry, A. 2018, "COSO's Updated Enterprise Risk Management FrameworkA Quest For Depth And Clarity", *Journal of Corporate Accounting and Finance,* vol. 29, no. 3, pp. 16-23.

Santesmases Mestre, M. 2009, *Dyane versión 4 : diseño y análisis de encuestas en investigación social y de mercados / Miguel Santesmases Mestre,* Madrid : Pirámide, Madrid.

Shetty, S., McShane, M., Zhang, L., Kesan, J.P., Kamhoua, C.A., Kwiat, K. & Njilla, L.L. 2018, "Reducing Informational Disadvantages to Improve Cyber Risk Management†", *Geneva Papers on Risk and Insurance: Issues and Practice,* vol. 43, no. 2, pp. 224-238.

Sierra Bravo, R. 2007, *Técnicas de investigación social : teoría y ejercicios / Restituto Sierra Bravo,* 14ª ed. 4ª reimp. edn, Madrid : Paraninfo, Madrid.

Taleb, N.N. 2007, "The 'black swan' (The 'Black Swan - The Impact of the Highly Improbable', Gregg Easterbrook's review)", *New York Times Book Review,* , pp. 4.

Tyson, D. 2007, *Security Convergence: Managing Enterprise Security Risk,* Elsevier.

Will M. Bertrand, J. & Fransoo, J.C. 2002, "Operations management research methodologies using quantitative modeling", *International journal of operations & production management,* vol. 22, no. 2, pp. 241-264.