AGERS

II PREMIO INTERNACIONAL DE INVESTIGACIÓN EN

GERENCIA DE RIESGOS

PREMIO JULIO SÁEZ GARRIDO

APROXIMACIÓN A LA GERENCIA DE RIESGOS OPERACIONALES: IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD Y MEDIO AMBIENTE.

APUNTES PARA UN ANÁLISIS VECTORIAL DEL RIESGO Y PROPUESTA DE METODOLOGÍA DE EVALUACIÓN MIXTA POR PUNTOS

JOSÉ MARÍA CORTÉS SAAVEDRA.

MADRID ENERO DE 2011

NOTA: ESTA OBRA HA SIDO FINALISTA (2º LUGAR) DEL II PREMIO INTERNACIONAL DE GERENCIA DE RIESGOS "JULIO SÁENZ CASTILLO", PATROCINADO POR LA ASOCIACIÓN DE GERENTES DE RIESGOS ESPAÑOLES (AGERS) Y EL CENTRO DE SEGUROS DEL CORTE INGLÉS, SEGÚN FALLO DEL JURADO DE 12 DE MAYO DE 2011.

ESTE TRABAJO HA SIDO PRESENTADO POR MAPFRE, JUNTO A OTRA DOCUMENTACIÓN, AL XVI PREMIO INTERNACIONAL DE INVESTIGACIÓN EN SEGURIDAD (I+D) CONVOCADO POR LA EDITORIAL BORRMART, OBTENIENDO MAPFRE EL PRIMER PREMIO DE INVESTIGACIÓN EN SEGURIDAD.

A mi familia, Marivi y los niños, que me animaron a continuar

y hasta me corrigieron algún capítulo.

A mis padres y hermanos, que aún en la distancia y desde el Cielo,

siempre me apoyan.

A los amigos y compañeros de MAPFRE, en particular de la DISMA,

que han confiado en mí y me han alentado siempre.

A los amigos que me han empujado

y hasta han colaborado en este trabajo.

INDICE

RESUMEN

Es conocida la creciente preocupación por gestionar los riesgos operaciones, lo que se refleja en diversa normativa de aplicación en el sector bancario (Acuerdos de Basilea) y en el asegurador (Directiva de SOLVENCIA). Dentro del conjunto de riesgos operacionales, se encuentran los que pueden englobarse como riesgos de seguridad y de medio ambiente. Se trata de áreas de riesgo que, actualmente, se encuentran un tanto alejadas de los sistemas de gestión de riesgos de las empresas. Este trabajo analiza la situación de la gestión de los riesgos de seguridad y medio ambiente, estableciendo un paralelismo con la gestión del riesgo operacional en general. Se proponen pautas o líneas para implantar un sistema de gestión de riesgos de seguridad y medio ambiente, que posibiliten el aprovechamiento de sinergias y la coordinación con el resto de áreas de riesgo de la empresa, lo que redundará en el logro de una auténtica gestión integral de riesgos.

Como parte decisiva de la gestión de riesgos, se presta especial atención al análisis y evaluación de riesgos de seguridad y medio ambiente. Por este motivo se analizan empíricamente algunos de los métodos generales más significativos para evaluar estos riesgos, extrayendo conclusiones sobre su eficacia. A la par, se sacan conclusiones sobre la evaluación en general del riesgo operativo. Obteniéndose resultados no muy alentadores.

Con la vista puesta en la propuesta de una metodología de evaluación, que supere los inconvenientes encontrados en los métodos disponibles, se analiza previamente el concepto de riesgo. Se aborda este estudio conceptual desde la óptica matemática, centrándose sobre todo en la posible valoración estocástica de la probabilidad, en un intento de obtener herramientas o verificar su aplicabilidad para la cuantificación de los riesgos de seguridad y medio ambiente. Se llega a la conclusión de la casi imposible obtención de un valor probabilístico para estos riesgos, lo que nos lleva a la necesidad de considerar las evidencias o factores de riesgo, como aspectos decisivos para su cálculo. Buscamos entonces un método estadístico que permita

integrar las evidencias, lo que nos lleva considerar la aplicabilidad de la Inferencia Bayesiana a nuestro caso. Metodología que, al menos para nuestro caso, ha devenido también difícilmente aplicable.

Ante esta situación se ha optado por diseñar una metodología de evaluación específica que supere en la medida de lo posible los inconvenientes encontrados.

Como primera opción se ha efectuado una aproximación conceptual al riesgo desde el espacio vectorial, así se ha considerado el riesgo como vector. Desde esta posición se ha llegado a una definición del riesgo integradora de todos los factores y evidencias que se estimen. Se ha comprobado que las representaciones gráficas o mapas de riesgo, mediante el concepto vectorial del riesgo, adquieren una nueva dimensión, facilitando su compresión y la visualización del valor del riesgo e incorporando el parámetro de la dirección del riesgo, muy útil para la toma de decisiones.

Desde el concepto vectorial del riesgo, se ha desarrollado una metodología vectorial de evaluación de riesgos. Para comprobar su eficacia se ha utilizado el mismo método experimental con el que se analizaron los otros métodos. El comportamiento ha sido excelente.

No obstante, con la pretensión de disponer de un método de evaluación directamente aplicable y mecanizable, que superase la carga subjetiva, a partir de la consideración de todas las evidencias, factores de riesgos, vulnerabilidades y amenazas posibles; y además permitiese la cuantificación de los riesgos, se ha diseñado un segundo método para evaluar los riesgos de seguridad y medio ambiente. En este caos se ha optado por un método mixto con un sistema de puntos.

El método de evaluación mixto por puntos, desarrollado, parte de una potente check list, que posibilita la identificación de un amplio espectro de riesgos y situaciones que pueden influir en estos. Posibilita su automatización de forma sencilla, mediante la aplicación informática adecuada. Se ha diseñado un algoritmo para relacionar cada cuestión del Check List con todos y cada uno de los riesgos, lo que lleva automáticamente a disponer de un análisis de riesgos

muy detallado, incluyendo en el mismo una evaluación cualitativa. Finalmente, se ha diseñado un sistema de cálculo de los riesgos, mediante puntuaciones en función de la calificación obtenida para los riesgos primarios o para cada factor de riesgo. La herramienta informática adecuada, permite la automatización de todo el proceso, incluyendo la valoración final de los riesgos, informes de riesgos en función de sus características y su representación gráfica.

El método mixto por puntos para evaluaciones de seguridad y medio ambiente, es susceptible de aplicarse a otros ámbitos de riesgo. Supone una herramienta óptima para evaluar eficazmente los riesgos, siendo su implantación muy sencilla, sobre todo considerando su facilidad para ser directamente informatizado.

ABSTRACT

It is well-known the increasing concern to manage the operational risk, clearly reflected in the varied available regulations applicable to the bank (Basilea Agreemtns) and insurance (SOLVENCIA Directive) sectors. Risks that can be embraced as safety and environment risks are included inside the operational risks group. They represent risk areas which currently are quite away from company manage risk systems. This work analyses the safety and environment risks management, establishing a parallelism with the general operational risk management. Some guidelines and patterns are proposed in order to introduce a safety and environment risks management system, allowing the exploiting of the synergies together with the coordination with the rest of company risk areas, benefiting the achievement of a real integral risk management.

As a decisive part of risk management, special attention is paid in the analysis and evaluation of the safety and environment risks. For this reason, several of the most general risk evaluation methods are empirically analyzed to evaluate them, drawing conclusions about their effectiveness. General operational risks evaluation conclusions are also identified, with not very encouraging results.

Trying to propose an evaluation methodology to solve the disadvantages coming from the available methods, this work first analyzes the risk concept. This conceptual study is tackled by the mathematic viewpoint, based specially in the possible stochastic assessment of the probability, trying to obtain tools or verifying their applicability for the quantification of the safety and environment risks. The main conclusion drawn is that it is not possible to obtain a probabilistic value for these risks, implying the necessity of consider evidence or risk factors as decisive aspects for the calculation. A statistical method is therefore used to allow us the integration of all evidence, hence considering the application of the Bayesian Inference to our case. This methodology has been difficult to apply, at least in our study.

In front of this situation it has been chosen to design a specific evaluation methodology to overcome, as much as possible, the problems found.

As a first option a conceptual approximation from vectorial space to the risk has been performed, considering therefore the risk as a vector. Starting from this position a risk definition has been created integrating the different factor and evidence used. It has been verified that, using this vectorial risk concept, the risk maps or graphical representations have acquired a new dimension, facilitating their comprehension and displaying the risk value, incorporating the risk direction parameter, very useful for the decision making issues.

From the vectorial risk concept, a vectorial risk evaluation methodology has been developed. In order to verify its effectiveness, the same experimental method used to analyze other methods has been used. The outcome behavior has been excellent. Nevertheless, in order to provide an evaluation method with direct and systematic application, going beyond the subjective view from the consideration of all evidence, risk factors, vulnerabilities and hazards, and allowing, at the same time, the risk quantification, a second method has been designed to evaluate the safety and environment risks. In this case a mixed point based method has been selected.

The mixed based point method selected starts from an integral and complete check-list, allowing the identification of a wide risk spectrum and different situation that may affect those risks. It easily allows the automation through a software application. A specific algorithm has been design to correlate each question included in the check list with all and each of the possible risks. With this approach a very detailed risk analysis is automatically obtained, including a qualitative evaluation as well. Finally a risk calculation system has been also designed, using specific punctuation based in the resulted qualification for the primary risks or for each risk factor. The adequately software tool perform all the process automatically, including the final risk evaluation, different kind of reports based in risk characteristics and graphic representation of outcomes.

The mixed based point method to evaluate the safety and environment risks can also be applied to other risk environment. It represents a optimal tool to evaluate the risks, requiring a very simple deployment, since it can be easily adapted with the software application.

INTRODUCCIÓN.

Estamos asistiendo a una preocupación creciente por el control de los riesgos de todo tipo y en todo ámbito. La época de crisis que estamos viviendo viene a acrecentar esta necesidad de control, sin poder olvidar tampoco otros acontecimientos de tristes recuerdos como los ataques terroristas o las catástrofes naturales, desgraciadamente de permanente y fatídica actualidad. El denominador común de todos ellos es que han provocado graves daños, irreparables en ocasiones y que no se habían prevenido, al menos, correctamente.

Ciertamente la preocupación por el riesgo no es una actitud nueva, podríamos incluso convenir que es innata al ser humano y por ende a todas sus actividades. Pero lo que sí puede considerarse como fenómeno novedoso, sin duda auspiciado también por las circunstancias a que nos hemos referido, es el grado creciente de esa preocupación, tanto en intensidad como en extensión, alcanzando a todos los riesgos posibles. En línea con esta preocupación, también se viene percibiendo la necesidad de aplicar procedimientos científicos y racionalizados para controlar los riesgos, con un matiz integrador de los mismos.

Así, la tendencia natural y lógica es considerar la gestión de riesgos como un proceso racional que debe alcanzar a todos los riesgos a que está expuesto un grupo u organización. No cabe por tanto excepcionar de los procesos de gerencia ninguna de las posibles áreas de riesgo, aún cuando respondan a naturaleza y causas diferentes.

Pero también resulta evidente que la gestión de riesgos de áreas o naturaleza concretas, deberá particularizase adaptando los procedimientos, métodos y herramientas de gestión a sus peculiaridades. Lo que no obsta para que dicha gestión responda y beba de las líneas de gerencia de riesgos establecidas por la organización así como de los estándares admitidos.

En este sentido, los riesgos que tradicionalmente se han considerado desde las áreas de seguridad patrimonial (término poco preciso como tendremos ocasión de ver) o corporativa de

las empresas, deben integrarse también en los sistemas de gerencia de riesgos de las mismas. Llevando a cabo, de acuerdo con el razonamiento anterior, las adaptaciones y particularizaciones necesarias del proceso de gerencia que la empresa haya establecido para el conjunto de todos sus riesgos.

En otro orden de cosas, dentro del proceso de Gerencia de Riesgos cobra especial relevancia la fase de evaluación, tanto es así que no se puede hablar de una verdadera gerencia si no se ha efectuado la evaluación de riesgos. Resulta evidente que sin conocer el riesgo, el daño que puede causar a nuestra organización, la probabilidad de que suceda y su causa, difícilmente va a poder combatirse o tratarse con alguna esperanza de éxito.

Con esta premisa, partiendo de la evaluación como espina dorsal de la gerencia, obligado es que, en aras del tratamiento óptimo, ésta se efectúe de forma idónea, adecuada y efectiva. Por este motivo el presente trabajo trata, esencialmente, sobre la evaluación de riesgos y las fases previas necesarias para llegar a la misma.

Centrándonos en las áreas de seguridad como órganos o departamentos de las empresas gestores de unos riesgos específicos y, podríamos decir, de naturaleza diferentes al resto, desde un análisis somero de la situación, se pueden obtener estas conclusiones:

- La seguridad, (mediante este término en lo sucesivo nos referiremos a lo que se conoce como seguridad patrimonial, corporativa o security, aun entendiendo que en estos conceptos no se agota su campo de actuación) se trata de un área de riesgo puro que, a pesar de ser pionera en el tratamiento de los riesgos, (esa es su razón de ser precisamente) ciertamente, está quedando descolgada de los modernos sistemas de gerencia que están adoptando las empresas, que tradicionalmente se han mostrado más centradas en otras áreas de riesgos como los financieros, los de negocio.
- Desde estas áreas de la seguridad o su entrono, se han desarrollado métodos propios de evaluación de riesgos (entre los más paradigmáticos cabría mencionar al método

Mösler), sin que, desde nuestro punto de vista, se haya avanzado lo suficiente en estas técnicas que por lo general adolecen de una elevada carga subjetiva y de haber sido diseñadas para casos muy concretos, con lo que devienen inaplicables para el resto.

- Se aprecia un cambio en las perspectivas de gestión de estos riesgos concediéndoles una importancia creciente, más acorde con su potencial gravedad y trascendencia para el devenir de la empresa. En esta línea es preciso mencionar las normativas sectoriales que constituyen la referencia de la gestión de riesgos en el ámbito bancario y en el asegurador (Acuerdos de Basilea y Directiva de SOLVENCIA, respectivamente). Incidiendo y concediendo una importancia sin precedentes a la gestión del riesgo operacional, categorización en la que, como se analizará en este trabajo, deben incluirse los riesgos tradicionalmente gestionados por las áreas de seguridad.

Todo lo expuesto hasta aquí, nos ha impulsado a centrar este trabajo en la gerencia de riesgos de seguridad, con la pretensión de diseñar y proponer líneas de acción precisas y prácticas, que sirvan de base para gestionarlos bajo los parámetros y procesos estandarizados de la gerencia de riesgos; posibilitando así su integración coherente con la gestión del resto de riesgos que afectan a la organización y el aprovechamiento de sinergias entre las diferentes áreas responsables de su gestión directa.

Diseñar y describir un proceso de gerencia con toda su amplitud y con el detalle necesario para alcanzar el nivel práctico que se pretende mediante le presente trabajo, excedería los límites y la finalidad del mismo. Esta circunstancia nos ha inducido a ceñirnos a la fase que consideramos más importante y crucial para abordar una auténtica gerencia, esto es a la evaluación de riesgos. Si bien no se limita estrictamente a la misma, abordando las otras fases previas y necesarias para valorar el riesgo, como son la identificación y el análisis.

Tampoco se ha desdeñado tratar asuntos necesarios y transversales a cualquier aproximación a la gestión de riesgos que se precie. Así se entrará en estudios conceptuales, incluso sobre la

misma naturaleza y formulación del riesgo. Delimitando en cualquier caso el campo de actuación de un proceso de gerencia de riesgos de seguridad.

De este modo, se ha optado por diseñar métodos prácticos y específicos aplicables a las áreas de seguridad, siempre bajo el paraguas de un proceso de gerencia estandarizado, enfocando nuestras propuestas al diseño de metodologías de evaluación aplicables a los riesgos de seguridad y medio ambiente.

Este enfoque hacia la seguridad, no será óbice para que, mediante las adaptaciones necesarias, la metodología propuesta pueda ser aplicable a otras áreas de riesgo, en particular a aquellas que se engloban dentro de los riesgos operacionales.

En un afán de dar respuesta concepto de *"Seguridad Integral"*, antecesor sin duda del actualmente pujante "*Gerencia Integral de Riesgos",* en los métodos propuestos se incluyen aspectos propios de la gestión de riesgos medioambientales. Sin duda, influenciados también por la cercanía y similitud de ambos procesos, lo que frecuentemente lleva a mencionar los riesgos de medio ambiente, junto a los de seguridad[1].

No obstante, es preciso matizar que por contraposición a la seguridad, desde el ámbito medio ambiental, se han desarrollado quizá los métodos de evaluación de riesgos más específicos y científicos. Contando también la rama de medio ambiente con sistemas específicos de gestión; adoleciendo, no obstante, de una falta de integración en los procesos o sistemas de gerencia de riesgos de las empresas. Aspecto este último que justifica con creces su referencia e inclusión en este trabajo junto a los riesgos de seguridad.

Concretando sobre la metodología de evaluación propuesta, se significa que se ha partido del examen detallado de algunos de los métodos generalistas, aplicables, en principio, a todo el

[1] No es novedoso un análisis conjunto de los riesgos de seguridad y medio ambiente; de forma conjunta, y además con los de seguridad laboral se abordan en la obra "Manual de Evaluación y Administración de Riesgos" de Rao Kolluru, Steven Bartell, Robin Pitblado y Scott Stricoff. Editorial Mc Graw Hill.

catálogo de riesgos[2], extrayendo conclusiones sobre su bondad. Para llevar a cabo estos análisis se ha utilizado un método experimental, planteando un caso ficticio, con riesgos evidentes e importantes a priori, sobre el que se han aplicado los distintos métodos de evaluación considerados. Se ha podido comprobar hasta qué punto los métodos analizados son aplicables al universo de riesgos de seguridad y medio ambiente; verificando si se trata realmente de métodos cuantitativos y objetivos, o por el contrario, en qué medida adolecen de apreciaciones subjetivas que devalúan los resultados. Finalmente, se ha tratado de comprobar si los resultados obtenidos responden a la realidad.

En el camino ha sido preciso fijarse en los mapas de riesgos como principal producto de la evaluación.

Como parte central del trabajo, se van a proponer metodologías propias para la Evaluación. En este sentido, como fruto de nuestras propuestas metodológicas se llegará a una relaboración de los mapas de riesgos.

En cuanto a las metodologías propuestas, se enfocan desde dos puntos de vista.

Por una parte, se esbozan unas ideas sobre la naturaleza del riesgo como concepto, lo que nos llevará a una formulación integradora y genérica. Como novedad se aborda el estudio del riesgo desde la perspectiva del análisis y el cálculo vectorial. Es necesario puntualizar que la pretensión de este análisis es conseguir un método práctico capaz de integrar múltiples factores de riesgo y de lograr su cuantificación, para ello se ha partido de criterios racionales y científicos. No se ha abordado el desarrollo científico completo de esta teoría que por su posible trascendencia (supone un enfoque del riesgo diferente al que se ha seguido de forma generalizada hasta ahora), quizá y si se considerase merecedora de ello, debiera ser objeto de estudios específicos que determinasen su validez científica.

[2] Esto ha llevado a descartar métodos para evaluar específicamente aspectos concretos de seguridad como el MESSERI o el GRETENER diseñados para la evaluación del riesgo de incendio y que no resultan aplicables al resto de riesgos.

Partiendo de esta formulación vectorial del riesgo se diseña un método de evaluación clásico, con una propuesta de valoraciones como modelo, siendo de vital importancia que la organización se pronuncie sobre su apetencia al riesgo y adopte estas u otras gradaciones que estime adecuadas para los factores.

Pero como ya ha quedado sentado, la idea central de este trabajo es lograr un método de evaluación eminentemente práctico, generalista y que elimine en lo posible la carga subjetiva.

El enfoque vectorial que se ha mencionado no garantiza su aplicación inmediata, en tanto en cuanto no se disponga de las reglas adecuadas y admitidas para graduar los aspectos o factores de riesgo. Fue esta constatación la que llevó a diseñar un segundo método que fuese de aplicación directa, y que además gozase del resto de atributos que le estamos exigiendo a un método de evaluación fiable y eficaz; esto es que elimine en lo posible la carga subjetiva del evaluador, que sea generalista, aplicable por tanto a una generalidad de situaciones e incluso áreas de riesgo diferentes, que permitiese la identificación, el análisis y evaluación de la mayor parte de los riesgos y vulnerabilidades presentes, como muy importante, que cuantificara los riesgos. Como valor añadido, se pretendía y se ha logrado, que el método diseñado fuese mecanizable aplicando la herramienta informática adecuada.

El desarrollo de este método de evaluación constituye la última parte del libro. Diseñando así un *" Método de evaluación mixto por puntos"* que parte de una identificación exhaustiva y comprensiva de la mayor parte de las situaciones posibles que pueden encontrarse en una instalación y que pueden originar un riesgo, o constituir un factor de riesgo, una vulnerabilidad o una amenaza.

El formato para llevar a cabo la identificación y su estructuración permiten su mecanización aplicando sencillas herramientas informáticas.

Mediante la construcción de un algoritmo que relaciona todas y cada una de las situaciones de riesgo detectadas con todos y cada uno de los posibles riesgos, aplicando nuevamente la herramienta informática adecuada, se obtiene un informe de análisis de riesgos.

Posteriormente se ha diseñado una metodología específica para cuantificar los riesgos detectados, lo que nos lleva, finalmente, ante una evaluación cuantitativa (mixta en realidad como veremos al desarrollarla) y que nos arrojará como producto tanto el mapa de riesgos de la instalación como diversos informes de riesgos en función de su gravedad o de las zonas afectadas; posibilitando priorizar de forma coherente, racional y rápida la toma de decisión sobre los tratamientos adecuados para controlar los riesgos.

Se significa que, dada la exhaustividad del método propuesto, partiendo de sus casi 600 cuestiones, permite identificar y valorar desde los riesgos tradicionales de seguridad (intrusión, robo, etc.), hasta riesgos cuya evaluación no es frecuente como el riesgo de daño a la imagen o el riesgo de incumplimiento legal (ambos en relación con la seguridad), así como posibles responsabilidades por daños a terceros. Todo lo anterior, que puede enmarcarse en el riesgo reputacional, entronca con los ***Sistemas de COMPLIANCE***. De igual modo se identifican, analizan y valoran riesgos como el de terrorismo, agresiones personales, daños a la información, daños al medio ambiente, riesgos de la naturaleza y otros derivados de la localización de la instalación y su proximidad a fuentes de riesgo externas.

Finalmente, volviendo al contenido del trabajo en sí, cabe añadir que se han incluido definiciones conceptuales, a veces aplicables al ámbito del riesgo en general, y otras al particular de la seguridad y medio ambiente, con la finalidad de arrojar alguna luz que contribuya a aclarar ciertas contradicciones en cuanto a su utilización e incluso sobre los conceptos mismos. Los efectos prácticos que persigue este documento hacen necesarias dichas aclaraciones o al menos, sentar nuestras posiciones de partida. En este orden de cosas cabe citar que uno de los puntos de partida ha sido delimitar el campo de competencia de lo que se

conoce como seguridad, adelantando un posible catálogo de riesgos de seguridad y medio ambiente incluyendo definiciones y posibles vulnerabilidades.

CAPÍTULO 1. LOS RIESGOS DE SEGURIDAD Y MEDIO AMBIENTE

1.1 Delimitación del universo de riesgos.

Desde la introducción misma se ha planteado la necesidad de delimitar el ámbito de riesgo al que nos vamos a referir, para esto quizá la primera cuestión que surge sea precisar qué se entiende por "seguridad", y, dada la amplitud del concepto, ¿a qué tipo de seguridad nos referimos?

La definición más universal que podemos encontrar de "seguridad", obviamente la encontramos en el Diccionario de la RAE, según el cual, es la cualidad de seguro, y sinónimo de certeza. A la par, se puede apreciar que la propia definición introduce diferentes acepciones especificando "seguridad jurídica", "seguridad social", etc. Continuamos por esta vía y vemos que define "seguro" como:

- Libre y exento de todo peligro, daño o riesgo.
- Cierto, indubitable y en cierta manera infalible.
- Firme, constante y que no está en peligro de faltar o caerse.
- No sospechoso.

…….

Esto nos indica, como apuntábamos, la amplitud del término seguridad; que, como ya induce la propia Academia de la Lengua, hay que precisar, especificando a qué tipo de seguridad nos referimos.

Podemos encontrar varios tipos de seguridad que responden al objeto de este estudio, pero también comprobamos que ninguno de estos es comprensivo de la totalidad de la materia; careciendo también de definiciones oficiales incluso para estas acepciones específicas de seguridad, así, podemos mencionar:

- Seguridad Patrimonial: No cubre la totalidad del espectro deseado puesto que deja fuera los posibles riesgos a las personas, (agresiones, secuestro, terrorismo, amenazas, etc.) y, dependiendo del alcance terminológico, puede considerarse que tampoco engloba los daños a intangibles (daño a la imagen, por incumplimiento legal; reputacional en suma).
- Seguridad frente a actos antisociales: Es evidente que no todos los riesgos que vamos a tratar se deben a actos antisociales, algunos pueden ser accidentales e incluso fortuitos. (riesgos de la naturaleza, escape de sustancia contaminante, daños no intencionados a la información, etc.).
- En general no nos sirven todas las acepciones de seguridad que supongan una limitación en cuanto a los activos a proteger. Además de los ejemplos relacionados, no cubren conceptualmente todo el ámbito de actuación posible de las organizaciones o áreas de seguridad parcelas como la seguridad del trabajo, seguridad contraincendios, seguridad de la información, etc.

Podemos concluir que no es fácil encontrar un término que con carácter general defina el ámbito de actuación de las organizaciones de seguridad, englobando todas sus posibles áreas de riesgo.

Con esto nos aventuramos a definir la seguridad como la condición conseguida cuando los activos están protegidos contra los riesgos. Comprendiendo por otra parte, el conjunto de medidas necesarias para alcanzar esa condición.

Por organización de seguridad de la empresa (o Seguridad Corporativa) se entenderá el área de la empresa destinada a la protección de los activos frente a los riesgos cuya responsabilidad le ha sido encomendada.

Así, llegamos a que la delimitación del campo de la seguridad a que nos referimos vendrá dada por los riesgos cuya gestión se encomienda tradicionalmente, y de forma más o menos generalizada, a las organizaciones de seguridad corporativa. Consecuentemente, vamos a

proceder a desgranar la tipología de riesgos que caerían bajo el paraguas de las áreas de que constituyen las propias empresas para proteger sus activos.

A modo de ejemplo y sin que se trate en ningún caso de un catálogo cerrado o númerus clausus, se identifican las siguientes áreas de riesgo como las tradicionalmente gestionadas desde Seguridad, o susceptibles de serlo:

- Riesgo de Incendio.
- Riesgos de la Naturaleza.
- Riesgo Antisocial.
- Riesgo Medioambiental.
- Riesgos derivados de daños o ataques a la información, incluso el derivado de incumplimientos de la normativa de protección de datos personales (LOPD).
- No es inusual que desde las Áreas de Seguridad se gestionen también las posibles emergencias y los Planes de Autoprotección para hacerles frente.
- Hay autores que incluyen también los riesgos de Seguridad Laboral[3], en la gestión general de la seguridad.
- Riesgos de incumplimiento de la normativa específica (Ley de Seguridad Privada, De Protección Contra Incendios, de Medio Ambiente, etc.).
- Incluso desde estas áreas se pueden gestionar planes de continuidad de negocio, en la medida en que desde las mismas se gestionen las áreas de riesgo que puedan poner en peligro dicha continuidad.

[3] Como se recoge en la Nota 1, a título de ejemplo, cabe mencionar que los riesgos de seguridad, de medio ambiente y de seguridad laboral se abordan de forma conjunta en la obra "Manual de Evaluación y Administración de Riesgos" de los autores Rao Kolluru, Steven Bartell, Robin Pitblado y Scott Stricoff. Editorial Mc Graw Hill.
En las obras o tratados de seguridad es habitual también encontrar la seguridad laboral entre las disciplinas gestionadas conjuntamente desde seguridad, así en el Manual para el Director de Seguridad. Editorial E.T. Estudios Técnicos, 1996. Y en la misma línea las Instrucciones Técnicas de Seguridad Integral de la Fundación MAPFRE Estudios, quizá la más completa recopilación sobre seguridad integral realizada en España, comprende todas las ramas de seguridad mencionadas.

Fig. 1. Áreas de Seguridad y Medioambiente.

Fuente: Elaboración Propia

1.2 Posible tipología de riesgos de seguridad.

Dentro del Sistema de Gestión de Riesgos, la empresa debe disponer del catálogo de riesgos identificados como posibles, considerando su apetencia al riesgo o nivel de riesgo que esté dispuesta a asumir. A la hora de elaborar este catálogo, desde la perspectiva de gestión integral, se habrán identificado también los riesgos cuya gestión sea responsabilidad de las áreas de seguridad y medio ambiente.

Desde las áreas de seguridad y medio ambiente, como gestoras directas de estos riesgos, se deberá realimentar el catálogo general de riesgos de la empresa, en lo que concierne a estos de seguridad y medio ambiente. La función como áreas gestoras directas de éstos implicará la necesidad de profundizar más en los mismos, tanto desde el punto de vista cualitativo como cuantitativo. Así el catálogo propio de riesgos de seguridad y medio ambiente alcanzará detalles de riesgo cuya gestión directa por el CRO de la empresa, sería poco efectiva, partiendo

de que sus cometidos deben responder más a una gestión general de todos los que afectan a la empresa, que al detalle de los de un área concreta.

La gestión directa del riesgo, implica su conocimiento exhaustivo, lo que se inicia indefectiblemente, con una identificación de riesgos lo más detallada posible. Mediante la aplicación de las sucesivas fases de la gerencia, teniendo en cuenta la política de riesgos, se decidirá si todos o parte de esos identificados deben ser tratados, controlados, trasferido o asumidos.

Comenzamos este capítulo con la pretensión de delimitar el ámbito de riesgo en el que se focaliza la seguridad y el medio ambiente, vamos pues a plasmar con cierta exhaustividad lo que puede constituir el catálogo de riesgos propio de la actuación de estas áreas.

Es necesario precisar que un catálogo de riesgos no puede nunca constituir una relación cerrada. Ha de tomarse como orientación, como punto de partida para "saber qué riesgos hay que buscar"; lo que no puede impedir que riesgos identificados pero no contemplados en el catálogo, dejen de tratarse, o al menos de analizarse. Más bien al contrario, disponer de un óptimo y efectivo método de evaluación, con una potente herramienta para identificar los riesgos, operará como factor de retroalimentación y revisión del catálogo.

A su vez, la actualización del catálogo de riesgos de seguridad, podrá desembocar en la revisión del catálogo general de riesgos de la empresa.

Posible Catálogo de Riesgos de Seguridad y Medio Ambiente.

- **Riesgo de Intrusión.** La intrusión, más que un riesgo en sí mismo, se trata de una condición "sine qua non" para que se manifiesten gran parte del resto de riesgos. Con esta consideración, se deben considerar por una parte las posibilidades de que se produzca una intrusión en las distintas áreas, así como la posibilidad de que a

partir de la estancia (autorizado o no) en un área concreta se pueda producir la intrusión hacia otras.

Por otra parte, además de identificar los posibles factores que posibiliten o favorezcan la intrusión en un determinado recinto, deberán identificarse aquellos riesgos dentro del propio recinto cuya probabilidad se va a incrementar en la medida en que se posibilite la intrusión.

A modo de ejemplo, analizando el perímetro exterior, las circunstancias de la fachada, puertas exteriores y ventanas pueden posibilitar la intrusión al edificio. A partir de ésta pueden manifestarse una serie de riesgos como hurtos en general, acceso, robo o hurto de información, agresiones, daños, etc. que no se trata de riesgos que se van a manifestar en la fachada, puertas o ventanas. Pero si identificamos una posible intrusión en una parcela donde se encuentran equipos de valor, además de esos riesgos se tendrá en cuenta la posibilidad de que se dañen, roben o hurten esos equipos.

- **Riesgo de Robo, Hurto o Atraco.** Pese a tratarse de tres acciones distintas que dan origen a tipos penales diferentes, se mantiene esta denominación conjunta considerando que la finalidad y efectos sobre el patrimonio (grosso modo) coincide en las tres, respondiendo también a los mismos factores de riesgo y vulnerabilidades.

- **Riesgo de Vandalismo.** Este riesgo está presente en muchas instalaciones, sobre todo en aquellas que están ubicadas en zonas socialmente conflictivas.

- **Riesgo de Sabotaje**. Es un riesgo que no debe descartarse nunca, ni aún en aquellos edificios o instalaciones en los que su frecuencia de manifestación sea escasa o prácticamente nula. La falta de control podría llevar a facilidades para su comisión, lo que incrementaría la posibilidad. Por otra parte, si se manifestase un riesgo de

este tipo, las consecuencias, por lo general, serán graves, pudiendo llegar a perturbar o impedir el funcionamiento de la instalación y, generalmente, el desarrollo de la actividad.

- **Riesgo de Incendio.** En algunos tratados se incluye dentro de los riesgos tecnológicos. Por nuestra parte, dada su importancia y trascendencia se analiza como riesgo independiente del resto de riesgos tecnológicos. Cabe significar que se trata del riesgo, que caso de manifestarse, estadísticamente, lleva en mayor número de ocasiones a la desaparición de la empresa. Estamos pues ante un riesgo extremadamente grave.

  Sobre este riesgo pende además una legislación y normativa muy prolija, lo que por una parte puede implicar el riesgo legal por incumplimiento de la misma, (este aspecto se analiza como riesgo independiente) y por otra, puede llevar a pensar que con su cumplimiento se elimina el riesgo de incendio, actitud esta última que constituiría un grave error, incrementando el propio riesgo.

- **Riesgo de Terrorismo.** Se trata de un riesgo cuya probabilidad está sujeta a circunstancias espacio - temporales. Su probabilidad será mayor en la medida en que la empresa cuente con edificios, instalaciones, personal o intereses en zonas geográficas afectadas en mayor grado por esta lacra. Así como en los casos en que la propia empresa o personal de la misma se encuentren directamente bajo esta amenaza. En estos casos se tratará de un riesgo muy grave, perfectamente identificable y para cuya gestión ha de contarse con el auxilio de las Fuerzas y Cuerpos de Seguridad, con los que debe reforzarse la colaboración. Sin que su carácter de riesgo público, como muy dañino para toda la sociedad, pueda llevar a la inhibición de la empresa en su gestión.

Ha de considerarse también, de cara a su gestión, para aquellas empresas no incluidas entre las anteriores, es decir, las que no sufren una amenaza terrorista directa. La naturaleza y características del riesgo de terrorismo obligan a que no se descarte en ningún caso. En estos casos quizá no lleve a la necesidad de adoptar grandes medidas contraterroristas, pero siempre, en toda circunstancia, debe considerarse como posibilidad, identificando situaciones que facilitarían un atentado, proponiendo medidas de autoprotección para los directivos y procurando, en todo caso, la colaboración e intercambio de información permanentes con las Fuerzas y Cuerpos de Seguridad.

Dentro de este riesgo se han de considerar sus diferentes modalidades, desde el atentado contra el edificio, a la introducción de paquetes o carta bomba, pasando por el atentado personal y el secuestro.

- **Riesgo de Agresión y Amenazas.** Se trata de un riesgo que puede provocar un daño a las personas. De manifestaciónón relativamente frecuente, afectando tanto a los empleados con funciones de atención al público como a directivos; sobre todo en situaciones de conflictividad socio laboral. Se vincula con la seguridad en general que ofrece el edificio.

- **Otros riesgos a las personas, (extorsión, chantaje, amenaza, secuestro…).** Son riesgos cuya gestión forma parte del acervo típico de las áreas de seguridad. Son riesgos graves ya que ponen en riesgo a las personas, dañando y afectando a toda la empresa. El área de seguridad debe tener establecidos sus protocolos de actuación, medidas de autoprotección, etc. Para el control final de este riesgo, intervendrán las Fuerzas y Cuerpos de Seguridad y la Administración de Justicia, con las que desde el área de seguridad, se extremará la colaboración.

- **Riesgos personales, (fraude, estafa, infidelidad de empleados…).** El desarrollo de la gestión de este riesgo, sobre todo en su fase de control, guarda similitud con el anterior, precisando la intervención de las Fuerzas y Cuerpos de Seguridad y de la Administración de Justicia en última instancia. Dependiendo de la naturaleza y circunstancias de estos riesgos, pueden no recaer en su totalidad en las áreas de seguridad, pero se ha de considerar que siempre desde esta área puede colaborarse tanto para su prevención como para su mejor control y resolución.

- **Riesgos de la Información; vinculados a su daño, robo, hurto o acceso no autorizado.** Una parte de este riesgo se centra en los riesgos vinculados a la instalación o edificio, desde esta perspectiva se analiza el control de acceso a los equipos y a las fuentes de información, el control del soporte papel y las posibilidades de acceso sin control adecuado a los propios recintos. Esta gestión implicará verificar si se dispone y observan las medidas de seguridad adecuadas.

  Por otra parte, hay que considerar el propio riesgo tecnológico como acceso o daños a la información no autorizado con medios telemáticos. Constituye esta modalidad uno de los riesgos más actuales, cambiantes y graves, que sufren hoy en día las empresas. Su gestión y control exige un alta especialización e importantes recursos. El acceso, perturbación o daño a la información puede ser el origen de otros daños como importantes pérdidas patrimoniales, imagen o poner en riesgo la continuidad del negocio.

- **Riesgo Medioambiental.** Se considera como tal el que puede provocar un daño al medio ambiente. Se diferencia del riesgo de incumpliendo de la Normativa Medioambiental que se estudia como riesgo específico.

- **Riesgo de Incumplimiento Normativo: Medio Ambiente.** Se incluye tanto el posible incumplimiento de la Normativa Medioambiental, a todos los niveles, como

el incumplimiento del Sistema de Gestión Medioambiental establecido, así como de aquellos parámetros que van a impedir o dificultar la obtención de la Certificación Medioambiental.

- **Riesgo de Incumplimiento Normativo: Contraincendios – Plan de Autoprotección y Emergencias.** Se diferencia el riesgo de incendio del riesgo de incumplimiento normativo en esta materia. Entre este posible incumplimiento normativo se incluye la normativa de autoprotección y emergencias.

- **Riesgo de Incumplimiento Normativo: Seguridad Privada** La observación de la Normativa de Seguridad Privada, por lo general recaerá en la Organización de Seguridad de la empresa, como responsable directo de la Seguridad.

- **Riesgo Daños a Terceros que tengan su causa u origen en la instalación.** Se identificarán y analizarán las posibles situaciones que puedan derivar en la exigencia de responsabilidad civil o de otro tipo a la empresa, y que encuentren su causa u origen en el propio edificio o instalación o derivados de la permanencia en el mismo. La gestión de este riesgo pasa por su identificación y evaluación, previniendo las posibles causas, llegándose a su transferencia mediante el aseguramiento.

- **Riesgo de Imagen.** Se han de considerar todas aquellas situaciones que, en el ámbito de la Seguridad y el Medio Ambiente, puedan llevar a un deterioro, aún en grado mínimo, de la imagen de la empresa o de la marca. Este riesgo no se suele analizar desde la perspectiva de la seguridad, y en general, se trata de un riesgo de muy difícil valoración, pero cuyos efectos dañinos están admitidos de forma generalizada.

- **Riesgo Reputacional.** Categorización que engloba varios de los aspectos analizados anteriormente, como el riesgo de incumplimiento legal por diversas causas y el

riesgo de daño a la imagen. Como ya se ha especificado, si no en su totalidad, sí una parte del mismo puede gestionarse desde las áreas de seguridad y medio ambiente.

- **Riesgo de la Naturaleza.** Se incluyen aquí todos los riesgos cuyo origen son causas naturales. Gran aparte de estos están vinculados a la zona geográfica donde se ubique el edificio o la instalación (terremoto, inundación, tormenta, etc.). Quizá no sean riesgos propiamente de seguridad, pero pueden recaer en estas áreas considerando que sus efectos dañinos sí afectarán al nivel de seguridad del edificio y de las personas que albergue; concurriendo además que las empresas no suelen disponer de áreas para su gestión específica.

- **Riesgo Tecnológico Químico: Explosión.** Se ha diferenciado del incendio por su especificidad en cuanto a causas y consecuencias, si bien está unido a aquel dado que una explosión implicará también un incendio en muchos casos. En los edificios se puede identificar asociado a instalaciones de gas o combustible o por proximidad a instalaciones ajenas afectadas por estos riesgos.

- **Riesgo Tecnológico Físico: Eléctrico.** Este riesgo, que está presente en toda instalación, se considera en la medida en que una deficiente seguridad (generalmente en el control de accesos) puede facilitarlo. Por ejemplo si no se controla y restringe el acceso a un transformador, a los cuartos eléctricos o a las salas de máquinas.

- **Riesgo Tecnológico Físico: Mecánico.** En cuanto al riesgo mecánico cabe mencionar lo expresado anteriormente para el riesgo eléctrico. Se valorará por tanto este riesgo desde la perspectiva del acceso a recintos como las zonas de máquinas donde existe la posibilidad de que se produzcan estos daños. Identificando si se controla o no dicho acceso.

- **Riesgo Tecnológico: Radiaciones ionizantes o nucleares.** Este tipo de riesgo se considera posible en tanto en cuanto se disponga de equipos que emitan radiaciones. En las instalaciones que no desarrollen una actividad empresarial específicamente relacionada con la energía nuclear, generalmente se encontrará en muy baja medida. Está presente en equipos como los escáneres para inspección postal y de paquetería y en las clínicas que dispongan de determinados equipos médicos. Exigen una gestión específica, incluyendo la aplicación de normativas tanto ambientales como particulares para equipos radiactivos.

- **Riesgo Tecnológico: Radiaciones no ionizantes.** Radiaciones procedentes de determinados equipos o aparatos como microondas. De escasa incidencia.

- **Riesgo Técnico por Diseño o Estructura.** Como tales se consideran los riesgos cuyo origen haya sido un mal diseño de la instalación. No es un riesgo gestionado por seguridad, pero como su gestión se verá, generalmente, afectada por el mismo deben identificarse las situaciones deficientes del edificio que puedan implicar o facilitar la aparición de riesgos de seguridad, dificulten o impidan su control.

- **Riesgo Técnico: Inundación.** Se identifican situaciones que pueden llevar a este riesgo, bien por canalizaciones y conducciones de agua, bien por la climatología y el diseño de la instalación. Se debe evaluar especialmente en aquellas instalaciones críticas en las que una posible inundación implicaría graves daños e incluso dificultades para el desarrollo de la actividad. Cabe citar entre estas, los archivos o los centros de comunicaciones o informáticos.

- **Otros Riesgos de Origen Biológico que afectan a la Seguridad y al Medio Ambiente: Infección Alimenticia, Infección Bactericida.** Se incluyen aquí riesgos cuya gestión puede o no estar encomendada a Seguridad. Pero sobre los que no cabe duda que, caso de manifestarse, podría provocar daños importantes y

afectaría de un modo u otro a la seguridad pudiendo incluso incurrir la empresa en algún tipo de responsabilidad.

1.3 Los riesgos de seguridad y medio ambiente como riesgos operacionales.

En el ámbito de la gerencia de riesgos son escasas, por no decir inexistentes, las referencias expresas a los riesgos de seguridad como área aglutinadora a su vez del conjunto de riesgos que venimos analizando. Cuestión que tampoco ha de extrañar considerando que, como se ha puesto de manifiesto, no es fácil encontrar el término comprensivo de todos los riesgos que se gestionan o pueden gestionarse desde las áreas de seguridad.

Ahora bien, desde un tiempo relativamente reciente, desde el ámbito de la gestión de riesgos viene acuñándose el concepto de "Riesgo Operacional" o "Riesgo Operativo".

Hemos estimado conveniente analizar por una parte este tipo de riesgos y por otra, verificar su posible relación con la materia objeto de este trabajo: la gestión de riesgos de seguridad y medio ambiente.

1.3.1 El riesgo operacional en la normativa.

Tanto en el ámbito bancario como en el asegurador, viene concediéndosele gran importancia a la gestión de riesgos. Tanto que se han alcanzado acuerdos sectoriales al respecto y promulgado normativa específica con incidencia directa en la gestión de riesgos. El impulso desde estos dos sectores claves para la economía, opera indubitablemente, como motor de arrastre para la gestión de riesgos de todo el ámbito empresarial; así lo analizado desde aquí

sobre esta materia, aun referido a esos dos sectores concretos, bien puede extrapolarse al resto de empresas.

La normativa específica para el sector bancario y para el sector asegurador, materializada respectivamente por los ***ACUERDOS DE BASILEA*** y por la ***Directiva de SOLVENCIA II*** no dejan ninguna duda sobre la necesidad de gestionar y controlar todos los riesgos "presentes y futuros" a que pueda estar expuesta una entidad. El enfoque es integral, es decir, hay que controlar todos los riesgos, independientemente de su naturaleza.

Por otra parte, desde ambos cuerpos normativos, se concede especial atención al Riesgo Operativo[4], incluido en el conjunto de los riesgos a que pueden estar expuestas las entidades. Analizando lo que establece *SOLVENCIA II* al respecto constataremos la trascendencia creciente de la gestión de estos riesgos.

Es de sobra conocido que el grado de eficacia y el modelo que se adopte para la gestión de los riesgos va a incidir directamente en los recursos propios mínimos que se requerirán tanto a las aseguradoras como a las entidades financieras.

Así, como uno de los principales objetivos de *SOLVENCIA II* puede enunciarse el desarrollo de un nuevo sistema que permita **determinar los recursos propios mínimos** a requerir a cada aseguradora, **en función de los riesgos** asumidos **y de la gestión** que se realice de cada uno de ellos. Además, establece unos mecanismos para lograr la efectiva y eficiente gestión del riesgo y la verificación de esta gestión por parte del Supervisor.

Concretando sobre esta **función de gestión de riesgos**, *SOLVENCIA II* especifica que las empresas de seguros y de reaseguros deberán **disponer de un sistema eficaz de gestión de riesgos**, que comprenderá las estrategias, los procesos y los procedimientos de información

[4] La autora María Ángeles Nieto Giménez – Montesinos, en su trabajo "El tratamiento del riesgo operacional en Basilea II" (Banco de España. Estabilidad Financiera, núm 8. Pdf) pone de relieve la importancia creciente del riesgo operacional, verificado por el tratamiento como Pilar 1 que le da BASILEA II, por detrás del riesgo de crédito y muy por delante del riesgo de mercado en cuanto a los requerimientos de capital.

necesarios **para identificar, medir, vigilar, gestionar y notificar de forma continua los riesgos a los que, estén o puedan estar expuestas**, y sus interdependencias.

Finalmente, entre las áreas que deben cubrirse con la función de gestión de riesgos, menciona expresamente la correspondiente a la gestión del riesgo operativo.

La importancia que se otorga a la Gestión del Riesgo Operativo se aprecia también al mencionarlo expresamente, entre los riesgos que es necesario cubrir para calcular el capital de solvencia obligatorio.

Referente a lo que se considera Riesgo Operativo, cabe decir que tanto *BASILEA II*, como *SOLVENCIA II*, lo definen como el derivado de la inadecuación o la disfunción de procesos internos, del personal y los sistemas, o de sucesos externos. Incluye los riesgos jurídicos, pero no los riesgos derivados de decisiones estratégicas ni los riesgos de reputación.

SOLVENCIA no especifica qué áreas de riesgo se considerarían Riesgo Operacional. Sí lo concreta *BASILEA* mencionando entre éstas: Fraude Interno, Prácticas con Clientes, Productos o Negocios, Seguridad en el Puesto de Trabajo, Daños a Activos Materiales, Fraude, Incidencias en el Negocio, Fallos en los Sistemas.

Fig. 2. Función de Gerencia de Riesgos.

Fuente: Elaboración Propia

Llegados a este punto, se hace necesario desgranar la función o funciones de las Áreas de Seguridad para dilucidar si la naturaleza de los riesgos que se gestionan desde las mismas permite u obliga a encuadrarlos, en su totalidad o en parte, entre los operacionales. Si la respuesta a esta cuestión es positiva, deberá concluirse que la gestión de estos riesgos también debería tratarse bajo el prisma de *SOLVENCIA II* en las aseguradoras o de los acuerdos de *BASILEA* en la banca. Conclusiones que podrían hacerse extensivas para el resto de empresas, como reflexiones para una gestión integral de sus riesgos.

1.3.2. ¿Son los riesgos de seguridad y medio ambiente riesgos operacionales?

Para contestar a este interrogante, debemos remitirnos a lo que se entiende por "Riesgos de Seguridad y Medio Ambiente", según lo recogido en este mismo capítulo.

No entra en nuestro ánimo repetir lo que ya se ha dicho en esa parte, únicamente con ánimo de centrar aquí el tema, conviene recordar algo de aquello.

Así, ya quedó sentado que bajo el concepto de riesgos de seguridad y medio ambiente, se engloban todos aquellos riesgos que tradicionalmente son gestionados por esas áreas. El catálogo de riesgos que se enumeraba podría incluirse en las áreas más generales de riesgo de incendio, de la Naturaleza, antisociales, medioambientales, riesgos derivados de daños o ataques a la información, riesgos gestionados mediante los Planes de Autoprotección susceptibles de provocar una emergencia, e incluso, como vimos, podrían alcanzar hasta los riesgos de Seguridad Laboral[5].

A la vista de la naturaleza de estos riesgos, para dar respuesta al interrogante planteado, cabe preguntarse cómo y en qué medida pueden afectar a una empresa.

En este sentido, no cabe duda de que afectan decisivamente a las empresas y que una deficiente gestión de los mismos, podría acarrearles graves y hasta irreparables daños. A modo de

[5] Ver Nota 3.

ejemplo, traemos a colación lo ya comentado en cuanto al riesgo de incendio, referente a que estadísticamente es el riesgo con más probabilidad de abocar a una empresa a su desaparición. Y a nadie se le escapa qué puede suponerle a una gran empresa, hablamos de su evolución, un atentado terrorista o el secuestro de un directivo. Como tampoco puede ignorarse que los riesgos relacionados con la información y los sistemas son muy frecuentes y especialmente dañinos, una caída en los sistemas de información puede provocar la paralización de la empresa o una parte del negocio, si no está bien controlado este riesgo.

Hay que considerar también que la práctica totalidad de estos riesgos, además de pérdidas patrimoniales y / o personales, y por pequeñas que sean éstas, van a implicar daño de imagen, a veces difícil de reparar.

Todo esto lleva a considerar que estamos ante riesgos muy importantes y decisivos para el desarrollo de la empresa.

Por lo anterior, y teniendo en cuenta que el objetivo de SOLVENCIA, coincidente con BASILEA, que aboga por la gestión integral de "todos los riesgos, presentes y futuros que afecten a la aseguradora", queda claro que esa necesidad de eficiente gestión alcanza también a los riesgos de seguridad y medio ambiente cuya responsabilidad recae en la Unidades de Seguridad.

Sentada la necesidad de gestionar los riesgos de seguridad y medio ambiente a la par que el resto de riesgos que vienen considerándose bajo el paraguas de SOLVENCIA y BASILEA, su encuadre dentro de las categorías o áreas de riesgo que ha de tratar la función gerencia, no puede ser más que dentro de los riesgos operacionales.

En este sentido, tal y como se ha visto, gran parte de las áreas de Riesgo Operacional que concreta BASILEA (Fraude Interno, Seguridad en el Puesto de Trabajo, Daños a Activos Materiales, Fraude, Incidencias en el Negocio, Fallos en los Sistemas) pueden encuadrarse en seguridad. No obstante, y pese a esta referencia, la normativa es cicatera a la hora de mencionar los riesgos de seguridad en conjunto, entre los operacionales.

Si bien cabe precisar que a la vista del catálogo expuesto para seguridad y de la propia definición de riesgo operativo, no todos cabrían en esta categoría, así el riesgo reputacional (en su vertiente de daño a la imagen). Ahora, la empresa debe también plantearse su gestión ya que es un riesgo importante y frecuente, independientemente de que se trate o no de un riesgo operativo. Esta gestión entronca con los sistemas de COMPLIANCE y buen gobierno también de ascendiente importancia para el desarrollo de la empresa.

Correlación entre las áreas de riesgo operacional (según Basilea) y las áreas de seguridad, con su posible afectación a la empresa.

BASILEA II	ÁREAS DE SEGURIDAD	AFECCIÓN A LA EMPRESA
Fraude Interno Prácticas con clientes, productos y negocios Daños a activos materiales	Seguridad Patrimonial. Seguridad Contra Incendios. Seguridad de la Información. LOPD Emergencias. Terrorismo. Medio Ambiente Riesgos de la Naturaleza. Continuidad del negocio	Pérdida Patrimonial Pérdida de Negocio y Oportunidades. Conflictividad Laboral
Relaciones laborales y seguridad en el puesto de trabajo	Seguridad de las Personas (frente a riesgos de agresiones, secuestros, amenazas, robos y hurtos personales, etc) Riesgos de la Naturaleza. Medio Ambiente	Pérdida Patrimonial Pérdida de Negocio y Oportunidades. Conflictividad Laboral
Fraude Externo e Incidencias en el negocio y fallos en los sistemas	R. Ataques a la Información	Pérdida Patrimonial Pérdida de Negocio y Oportunidades. Conflictividad Laboral

Fig. 3. Riesgo Operacional y Áreas de Seguridad.

Fuente: Elaboración Propia

.

CAPÍTULO 2. APROXIMACIÓN A LA GERENCIA DE RIESGOS DE SEGURIDAD

2.1. Análisis de la situación actual de la gestión de los riesgos de seguridad y medio ambiente y su relación con la gestión del riesgo operativo.

2.1.1. Gestión de riesgos desde las áreas de seguridad

Independientemente de la existencia o no en la organización de un modelo de gerencia implantado, las organizaciones de seguridad, respondiendo a su principal función dentro de la empresa, se han centrado en el control efectivo de estos riesgos mediante la implantación de medidas de seguridad, preventivas y reactivas.

Si bien es cierto que la gerencia como proceso completo no alcanza aún una implantación significativa en el ámbito de la seguridad, sí se ha de reconocer el camino que llevan recorrido en cuanto a identificación y análisis de los riesgos, como hitos necesarios para realizar un control efectivo y eficiente de los mismos.

En cuanto a la evaluación de estos riesgos de seguridad, en general, se encuentra con los mismos problemas que el resto de riesgos operacionales, básicamente con la dificultad para su cuantificación. Pese a esto, en el ámbito de la seguridad se cuenta con metodologías de evaluación más o menos científicas, pero desarrolladas en el aspecto teórico más que enfocadas hacia su aplicación práctica; adoleciendo de una gran carga subjetiva en general. Lo que abocan a que en la realidad su aplicación práctica quede muy limitada.

Este aspecto va a ser analizado en este mismo trabajo, valorando la eficacia práctica de algunos de los métodos de evaluación más representativos, mediante la aplicación de un método empírico.

No puede perderse de vista que un proceso de gerencia de riesgos de seguridad y medio ambiente, deberá contemplar, además de las fases ya mencionadas, el proceso de toma de decisión que posibilite decidir entre la conveniencia de adoptar medidas de control, la transferencia de riesgos o incluso la posibilidad de asumirlos.

Lógicamente, para cerrar este ciclo será necesario evaluar costes y riesgos, incluyendo la valoración de los activos, como condición sine qua non para calcular el posible daño.

2.1.2. La transferencia de riesgos de seguridad y medio ambiente.

Se ha mencionado la posibilidad de transferir los riesgos. Ciertamente, un proceso de gerencia que se precie debe incluir también esta fase, por lo que se hace necesario considerar la posibilidad de asegurar o transferir mediante algún mecanismo, también los riesgos de seguridad y medio ambiente.

Ahora bien, si se analiza la gestión del riesgo que se realiza desde las áreas de seguridad, es fácil concluir que son completamente ajenas a su transferencia, salvo alguna excepción.

Para desarrollar también esta fase de la gerencia, es necesario contar con personal experto en gestión o gerencia de riesgos y / o en seguros, personal no habitual en las unidades de seguridad. Circunstancia que por otra parte no representaría más problema que incorporar a profesionales de estas características o apoyarse en otras áreas de la empresa, expertas en esta materia.

Pero fuese cual fuese la solución que se adoptase, conviene hacer hincapié en que la gestión del riesgo en toda su extensión debe considerar también su posible transferencia. Sin perder de vista que para transferir el riesgo de seguridad y medio ambiente de forma óptima y eficaz, esta fase debe incardinarse en el conjunto del proceso de gerencia.

Esta última afirmación se hace considerando la relación estrecha que debe existir en cualquier caso entre las Unidades de Seguridad, como auténticos expertos en los riesgos de su

competencia, y las que, desde dentro o externas, tengan la responsabilidad de su aseguramiento o cualquier otra alternativa de transferencia. A modo de ejemplo, en general y desde el punto de vista metodológico, no se puede concebir la transferencia sin la valoración del riesgo para la que habrá que contar con su gestor directo, o sea, en nuestro caso, con la Unidad de Seguridad. Debiendo tener en cuenta, por otra parte, que la adopción de medidas de control preventivas pueden tener repercusión directa en el aseguramiento; por ejemplo, modificando la prima, o, de igual modo, si mediante aquellas se logra reducir el número de siniestros. Aspectos que en los que la labor de seguridad es decisiva.

2.1.3. Breve esbozo de la relación entre la gestión del riesgo operativo y la seguridad.

Si se analiza la gestión del riesgo operativo que, generalizando, se viene realizando en las empresas, se puede extraer lo siguiente:

La gestión del Riesgo Operativo, en las empresas, habitualmente se encuadra junto a la gestión del resto de riesgos, próximo a las áreas financieras y económicas o incluso a las de auditoría.

Acorde con su propio concepto, entre los riesgos operacionales suelen incluirse los derivados de la Gestión Administrativa, de Recursos Humanos, Comisiones, Comerciales, Atención al Cliente, Tecnológicos, etc. No es habitual contemplar, entre estos, los riesgos de seguridad al menos en toda su extensión, ni incluso los de medio ambiente; más allá de meras referencias puntuales en los cuestionarios de riesgo, sobre todo en cuanto a los riesgos de información. Y desde luego no suelen incorporarse al conjunto de la gestión del riesgo operativo, mediante procesos de gerencia implantados y coordinados.

Lo anterior no deja de parecer un tanto contradictorio teniendo en cuenta la importancia de estos riesgos de seguridad y medio ambiente en el conjunto de riesgos de la empresa, a lo que

cabe añadir la obligación legal de controlar todos los riesgos de forma integral, en particular en los ámbitos mencionados de la banca y seguros, con tendencia a su generalización.

Menos suele considerarse la gestión que tradicionalmente se viene haciendo desde esas otras áreas de riesgo, en pos de esa auténtica gerencia integral demandada por la normativa y de la optimización de recursos que pasa por el aprovechamiento de sinergias, entre las diferentes áreas que gestionan riesgos.

Se puede constatar que desde las áreas responsables de la gerencia de riesgos en las grandes empresas se es consciente de esta situación y de la importancia de estos riesgos. Cabe entonces preguntarse el motivo por el que la relación de éstas con las unidades de seguridad, se limita las más de las veces a meras colaboraciones puntuales, sin llegar a abordar auténticos procesos de gerencia también para los riesgos de seguridad y medio ambiente y sin incluirlos en la gestión del resto de riesgos de la empresa.

La respuesta puede venir desde varias partes. Por un lado puede estar motivado por el desconocimiento que se tiene, en la empresa en general, de sus propias unidades de seguridad; a lo que contribuye la necesaria confidencialidad que envuelve muchos de los asuntos tocantes a seguridad, unido a que son riesgos muy específicos y, por lo general, graves, lo que lleva a que sean tratados por personal muy especializado y quizá un tanto endogámico. Pero, curiosamente, por otro lado, estas mismas características casi pueden aplicarse también a las unidades sobre las que recae la gestión del resto de riesgos en las empresas. El resultado es que la posible colaboración entre estas áreas, funcionalmente alejadas, puede resultar a priori difícil y casi "contra natura". Dificultades que habrá que superar en aras de una colaboración que se hace necesaria para gestionar adecuadamente los riesgos.

2.3. Consideraciones para una integración real de riesgos.

Parece claro que es necesario aunar esfuerzos y aprovechar las sinergias entre las diferentes áreas con responsabilidad en la gestión de riesgos en las empresas, procurando así una efectiva gerencia integral, superando las dificultades funcionales y de cualquier tipo que dificulten esta colaboración.

Como se ha visto, desde SOLVENCIA se establece la necesidad de contar con una política de gerencia de riesgos. Disponer de esta Política, aplicable a todas la áreas de riesgos, es requisito necesario para abordar un proceso de gerencia coherente con los principios empresariales y con la apetencia del riesgo de la organización.

Por otra parte, se observa que muchos de los términos habituales en gerencia de riesgos, ya sea en las áreas financieras, en las de negocio, en las de operacional o en las de seguridad, no responden a los mismos conceptos. Esta situación provoca cierta confusión, dificultando el establecimiento de criterios y procedimientos comunes. Se estima importante unificar criterios conceptuales al menos a nivel de la misma organización, siendo deseable que esta unificación alcanzase niveles superiores extendiendo su aplicación a todo un sector y por supuesto lo óptimo sería que en el ámbito de la gerencia de riesgos se utilizase un lenguaje común.[6]

No se cuenta con procedimientos para evaluar el riesgo operacional en toda su extensión.
Las Directivas analizadas no establecen criterios específicos para llevar a cabo esta valoración; valoración que por otra parte consideran imprescindible.

En el mundo de la gerencia de riesgos en general no es fácil encontrar modelos genéricos para llevar a cabo una evaluación cuantitativa del riesgo operacional.

[6] En este sentido cabe citar positivamente el intento de unificación conceptual que supone la Guía ISO/CEI 73 "Gestión de Riesgos. Terminología. Líneas Directrices para el uso en las normas." Terminología adoptada por AGERS y FERMA. Sin que hasta la fecha se haya apreciado su implantación generalizada.

Esta situación lleva a considerar la necesidad de abordar o profundizar en el estudio o diseño de procedimientos de evaluación del riesgo operacional en toda su extensión, que lleguen incluso y en tanto en cuanto sea posible, a la cuantificación del riesgo.

Bases de datos de incidentes derivados del Riesgo Operacional.

SOLVENCIA también establece la necesidad de contar con estadísticas fiables y adecuadas para efectuar los cálculos de riesgo. Pero la realidad es que, en general, no se dispone de estadísticas de riesgos operacionales de cierta entidad y con la fiabilidad necesaria.

Sería conveniente disponer de estas bases de datos, tanto a nivel sectorial de las empresas de seguros, como a un nivel más amplio o intersectorial.

Proceso de Gerencia de Riesgos

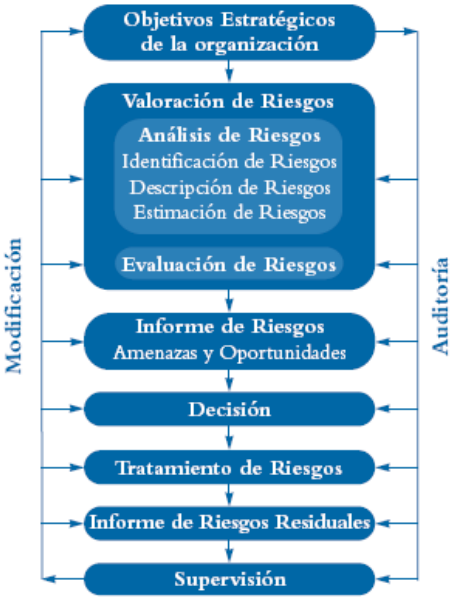


Fig. 4. Estándares de Gerencia.

Fuente: FERMA..

2.5 Modelo de gerencia de riesgos de seguridad y medio ambiente

Llegados a este punto, una vez centrado el ámbito de riesgo en que nos movemos, y analizada la situación bajo la óptica de la gerencia de riesgos, desembocando en ciertas consideraciones para alcanzar una gestión integrada de todos los riegos que pueden afectar a una empresa, obligado es que nos aventuremos a concretar unas ideas, quizá básicas pero esenciales, para el diseño de un modelo de gestión de riesgos de seguridad y medio ambiente que facilitase su integración con la gestión de riesgos integral.

Realmente, las líneas de la gerencia ya están tratadas y admitidas casi de forma generalizada. Así nuestra propuesta, no puede por menos que partir de esas premisas, profundizándolas y particularizándolas para nuestra área de riesgo. Y tampoco puede pasar desapercibido, el hecho de que, dado que, hoy por hoy, las acciones de seguridad aún se consideran alejadas de la gerencia de riesgos, pueda resultar conveniente especificar este proceso para aquellas.

El punto de partida para diseñar un proceso de gerencia, es el estándar de gerencia admitido por FERMA. Vamos pues a particularizar sus fases para la gestión de la seguridad y el medio ambiente.

2.5.1. Política de Riesgos

El proceso de gerencia debe ser asumido por la empresa desde la cúspide, no en vano se configura como un instrumento de control, y no sólo asumido, sino que debe ser impulsado desde la más alta dirección. Es más, la gestión de riesgos debe formar parte de la cultura de la empresa; en este sentido cabe recordar que *SOLVENCIA* lo incardina en el ***Sistema de GOBERNANZA.***

Por otra parte, la empresa debe marcar las líneas básicas de la gerencia, y en particular decidirá cuál es su aptitud ante el riesgo y su apetencia. Esta cuestión que puede tener resonancias

meramente teóricas es crucial para la práctica de la gestión de riesgos. El gestor debe tener claro qué riesgos no puede tolerar la empresa o, por ejemplo, si la política asumida obliga a gestionar hasta niveles bajos de riesgo o de determinados riesgos. En esta línea deberá marcarse de antemano qué nivel de riesgo se está dispuesto a asumir, o cuáles hay que controlar, a qué precio o cuáles transferir.

De este modo, también la gestión de riesgos de seguridad y medio ambiente debe saber a qué atenerse en cuanto a la aptitud ante el riesgo. Bien es cierto que lo aconsejable es que se parta de una identificación que contemple todos los riesgos posibles, pero no es menos cierto que según se avance en las fases de gerencia, se hará más necesario contar con las directrices de la empresa al más alto nivel, en particular a la hora de tomar la decisión sobre el tratamiento y control de los riesgos.

A estas cuestiones debe responderse mediante la política de riesgos, que como ha quedado recogido, debe emanar desde el nivel jerárquico más alto de la organización.

Cuestión adyacente será si es necesario contar con una política específica para riesgos de seguridad y / o de medio ambiente o puede subsumirse ésta en la política general de riesgos de la empresa. Nuestra opinión al respecto es que aunque se cuente con una política de riesgos general, debe haber también un pronunciamiento expreso de la organización para los riesgos de seguridad. El motivo de esta opinión es la propia especificidad de estos riesgos que, aún acogiéndose a la política general de riesgos, debe contar con líneas específicas de gestión.

La política de riesgos de seguridad, podrá desde otra perspectiva, recogerse en otros documentos necesarios para la gestión de estos riesgos, estamos pensando en Planes Directores de Seguridad (que en realidad se trata más de políticas de seguridad que de auténticos planes) o en Planes Estratégicos de Seguridad y Medio Ambiente, etc. Siempre y cuando en estos documentos se recojan las líneas maestras para llevar a cabo la gestión, obviamente.

2.5.2. Identificación, Análisis y Evaluación De Riesgos

La identificación de riesgos y de las situaciones, fuentes o factores de riesgo, va íntimamente unida al análisis; tanto que estas dos fases suelen confundirse, utilizando indistintamente ambos términos y considerando frecuentemente la identificación subsumida en el análisis.

Pese a lo anterior, desde el punto de vista conceptual, ha de quedar claro que aunque se adopte un proceso unificado para la identificación y el análisis de riesgos, se trata de tareas diferentes.

La identificación se ciñe exclusivamente a constatar lo que se observa o se aprecia, sin emitir ninguna valoración. Se trata de información pura.

El análisis implica valorar cómo afecta al activo la situación detectada, si implica o no un riesgo relevante para el sistema, considerando además si las características y circunstancias internas y externas que rodean al activo, influyen en la manifestación del riesgo. Se trata de información elaborada o inteligencia.

La identificación debe ser exhaustiva, no debe descartar ningún riesgo posible, incluso debe constatar las medidas o medios adoptados que están controlando el riesgo.

El análisis tamizará la identificación, recogerá las situaciones, circunstancias y vulnerabilidades que implican un riesgo relevante.

La identificación de riesgos

En esta fase se identificarán de forma metódica y exhaustiva todos los riesgos posibles, presentes y futuros así como las situaciones que puedan influir en los mismos.

Por un parte se recogerán datos de fuentes documentales y de las informaciones disponibles. Por otra, como fuente principal de información se recogerán los datos de campo mediante una visita de inspección a la instalación o activo a evaluar.

Se deberá recopilar toda la información posible referente a la instalación que tenga relevancia para la Seguridad o en el Medio Ambiente.

A modo de ejemplo, y sin que constituya una lista cerrada, ni obligatoria en todos los casos, el equipo analista deberá disponer o tener la posibilidad de consultar, los documentos que se relacionan:

- ✓ Planes de Seguridad de la Instalación.
- ✓ Planes de Medio Ambiente e identificación de aspectos medio ambientales de la instalación
- ✓ Planes de Autoprotección y Emergencias.
- ✓ Auditorías de Seguridad, de Medio Ambiente, de Incendios, de LOPD, de Seguridad de la Información, etc.
- ✓ Documentación sobre los planes para implantar medidas de seguridad o para su ejecución.
- ✓ Informes particulares de riesgos que afecten a la instalación.
- ✓ Planimetría actualizada de la instalación.
- ✓ Antecedentes de incidentes. (del edificio, de la empresa en general, del entorno social, nivel delicuencial de la zona, antecedentes de incidentes en seguridad de la documentación, antecedentes de incidentes medio ambientales, de incumplimiento normativos, etc.)

Es muy importante concertar entrevistas previas con el Responsable de Seguridad y Medio Ambiente de la instalación, así como con los responsables de la implantación de medidas, medios y sistemas, tanto de Seguridad como de Medio Ambiente. Recogiendo sus informaciones relevantes.

Para facilitar la recogida de datos, sobre todo los de campo, es recomendable disponer de alguna herramienta tipo check list o cuestionario específico para seguridad y medio ambiente. La inspección será detallada, previamente estructurada y planificada. Se apoyará en los

responsables de la instalación, de forma particular en el Responsable de Seguridad y Medio Ambiente.

Los datos recogidos se plasmarán enel Check List, recomendándose la recogida documental también por otros medios como fotografías.

El Análisis de Riesgos

A partir de la información y datos obtenidos, se elaborará un documento de análisis de riesgos, en el que se recogerán los identificados que afecten a la instalación, a las personas o a las actividades, con sus causas, fuentes de riesgo y las vulnerabilidades detectadas; valorando la posibilidad de que se manifiesten y el daño a los activos, humanos y materiales.

El catálogo de riesgos constituirá la guía de los riesgos tipo que probablemente afecten a los activos identificados; sin que la identificación deba basarse exclusivamente en éstos, como si de una lista cerrada se tratase; ya que por la propia naturaleza cambiante de los riesgos, mediante la aplicación del Check List y el Análisis de Riesgos podrían detectarse otros no incluidos en ese catálogo y que no puedan descartarse.

La evaluación de riesgos como fase diferenciada del análisis.

El propio análisis de riesgos puede constituir en sí mismo o recoger una evolución cualitativa.

En tanto en cuanto no se disponga de un método de evolución efectivo y que permita llega a una valoración cuantitativa lo más objetiva posible, puede subsumirse ésta en el análisis.

Para ello deberán introducirse valoraciones que engloben probabilidad e intensidad o consecuencias e, imprescindiblemente, deberán establecerse prioridades de actuación.

Pero hay que dejar claro que este tipo de métodos no es lo más óptimo desde el punto de vista de la eficacia, tienen a su favor la rapidez y que solventan las dificultades ciertas que existen para disponer de métodos de evaluación cuantitativos que además se adapten a las necesidades específicas de seguridad. La solución pasará por el diseño de una metodología específica.[7]

En cualquier caso, para la fase de evolución, es necesario contar con una gradación o modelo para clasificar los riesgos en orden a su gravedad. Si no se puede llevar a cabo la comparativa de los riesgos analizados con la regla establecida para la organización, no se puede considerar que se haya efectuado la evaluación.[8]

Lo anterior hace necesario, por otra parte contar con el criterio de riesgos de la empresa, según hemos manifestado en el apartado correspondiente a la política de riesgos. Así, deberá marcarse previamente qué se considera riesgo grave, medio, bajo, etc. En la medida en que la parametrización esté bien definida, se reducirá la carga subjetiva redundando en una mayor fiabilidad del método adoptado.

2.5.3. Mapa de Riesgos

El mapa de riesgos constituye uno de los principales productos que se obtienen con la evaluación de riesgos. Se trata de la representación gráfica de los riesgos, clasificados en orden a su importancia de forma que permiten tomar la decisión en cuanto a la prioridad de su tratamiento.

[7] En este mismo trabajo se exponen dos metodologías de evaluación diseñadas específicamente para riesgos de seguridad y medio ambiente, extrapolables, mediante adaptación, al resto de riesgos operativos. Ver capítulos 5 y 6. La Guía ISO / CEI 73, menciona entre las características necesarias de la evaluación de riesgos que posibilite la comparación de éstos.

Para disponer del mapa de riesgos es recomendable cuantificar de alguna forma el riesgo o al menos parametrizar los valores de probabilidad e intensidad, de modo que permitan su posicionamiento en un eje de coordenadas.

2.5.4. Medidas de Control

Siguiendo el estándar de gerencia (Fig. 5.) tras la evaluación del riesgo se estará en condiciones de decidir cuál es el tratamiento más adecuado para mitigar o reducir el riesgo.

Más aún, disponiendo de un análisis detallado, máxime si contiene elementos valorativos y establece prioridades de actuación, pueden diseñarse ya las medidas de control.

La fase de diseño de las medidas de seguridad necesarias, deberá incluir su presupuesto.

De acuerdo, una vez más, con la política de riesgos de seguridad adoptada, puede ya decidirse si, a la vista de la entidad del riesgo, deben acometerse medidas de seguridad para controlarlo.

No es objeto de este estudio entrar al detalle de las medidas posibles de seguridad, esto constituiría materia para un tratado específico, pero sí creemos conveniente efectuar una somera pasada por estas, para centrar el asunto.

Cuando hablamos de medidas de seguridad, se entienden tanto las de índole organizativa, como la instalación de medios de seguridad física (vallado, estructura, rejas, puertas, etc.), electrónicos (alarmas de seguridad y contraincendios, controles de acceso, escáner, circuito cerrado de televisión, etc.), medios humanos (vigilancia, personal de seguridad), medios para seguridad de la información (software y hardware adecuados al nivel de seguridad requerido, normativa de acceso, autorizaciones, etc.), medios de control de alarmas, incidentes y señales (central para recepción de señales de alarma y de incendios, centro de control de incidencias informáticas y para control de accesos a red, etc.).

2.5.5. Transferencia de los Riesgos de Seguridad

Una vez más, la política de riesgos, marcará el nivel de riesgos a partir del cuál se optará por transferirlos. Entre las opciones de transferencia de riesgos, para esta área, se considerará su aseguramiento por lo general.

A la vista de la evaluación, incluso en ocasiones con la misma identificación, podrá decidirse qué riesgos o parte de los mismos hay que asegurar.

Como en cualquier proceso de gerencia, se diseñará un programa de seguros que incluya los ramos de los riesgos identificados en el catálogo y que sean asegurables. Entre estos cabe citar los de incendio, robo, daños en general, responsabilidad civil, de equipos informáticos, etc.

Mención especial hay que hacer al aseguramiento de los riesgos de medio ambiente, que pueden incluirse en las pólizas generales de daños por una parte, y por otra habrá que considerar las necesidades legales de aseguramiento vigentes.[9]

El control de la siniestralidad cobra vital importancia, tanto a la hora de diseñar el programa como para considerar los posibles efectos beneficiosos de las medidas de seguridad adoptadas.

2.5.6. Acciones para controlar la eficacia

El proceso de gerencia finaliza con el establecimiento de los mecanismos y protocolos necesarios para verificar el nivel real de control de los riesgos.

Puede llevarse a cabo mediante un proceso análogo al mencionado para identificar y analizar los riesgos. Retroalimentando a partir de este todo el proceso.

Se particularizará con informes de riesgo residual.

[9] Nos referimos a la Ley 26/2007, de 23 de octubre, de Responsabilidad Medioambiental que obliga al aseguramiento o a la constitución de garantías financieras en determinados casos.

2.5.7. Comunicación de riesgos.

Comenzamos diciendo que el proceso de gerencia era un proceso de control para el nivel más alto de la empresa. Esto lógicamente pasa por mantener los adecuados cauces de información de los riesgos. Para ello habrá que diseñar instrumentos ágiles y precisos que hagan llegar la información adecuada y oportuna a cada nivel jerárquico.

Para este fin son especial útiles los mapas de riesgo, ya que permiten una visualización rápida del nivel de riesgo. El resto de documentación de riesgos aportará la información hasta el detalle requerido.

2.5.8. Flujograma de Gerencia de Riesgos de Seguridad y Medio Ambiente

A continuación se representa el flujograma del modelo de gerencia de riesgos de seguridad y medio ambiente propuesto.

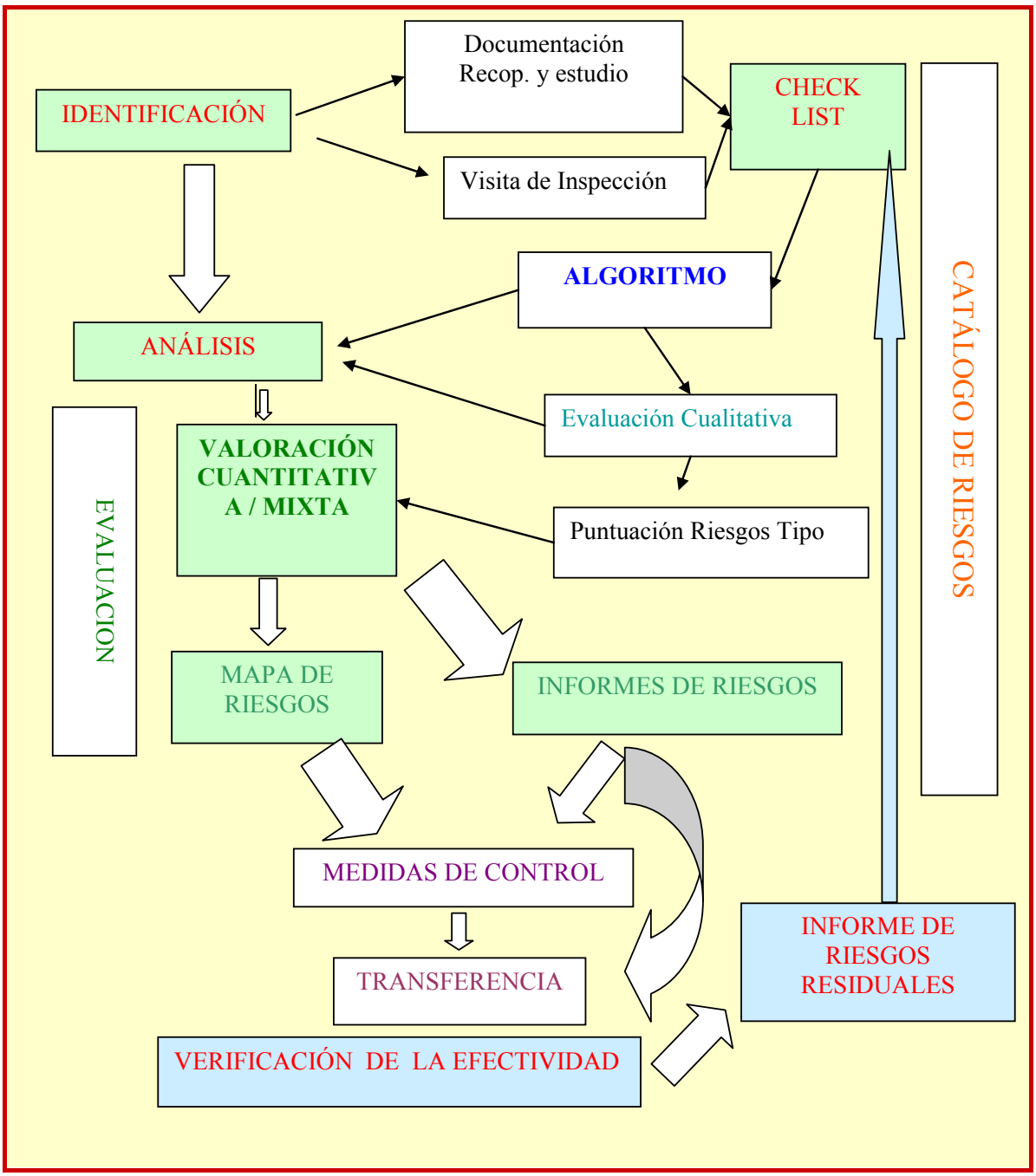


Fig. 5. Flujo de Gerencia de Riesgos de Seguridad.

Fuente: Elaboración Propia.

CAPÍTULO 3. ANÁLISIS EMPIRICO DE VARIOS MÉTODOS DE EVALUACIÓN DE RIESGOS EN EL ÁMBITO DE LA SEGURIDAD

Además de analizar la gestión de seguridad desde su alineamiento o no con los procesos de gerencia de riesgos, proponiendo ciertas líneas de actuación para su consecución, desde el principio ha quedado también clara la pretensión de analizar especialmente algunos de los métodos de evaluación de seguridad más representativos. La finalidad de esta parte del trabajo no es otra que dilucidar objetiva y asépticamente si la gestión de seguridad cuenta con métodos de evaluación realmente efectivos, suficientemente objetivos y que, en suma, sean óptimos para poder valorar estos riesgos de manera fiable.

Para ello nada mejor, desde nuestro punto de vista, que utilizar un método experimental comprobando su comportamiento frente a un caso tipo, sacando a flote sus posibilidades o imposibilidades de aplicación.

Métodos de evaluación de riesgos de seguridad hay muchos ya publicados e incluso algunos muy extendidos en este ámbito. No es necesario decir que el objetivo de este estudio no es analizar todos ellos, ni siquiera la mayor parte. La pretensión ha sido tomar algunos de los más representativos de aplicación generalista, volcando sobre estos nuestra disección.

Se ha mencionado que se parte de métodos generalistas. Efectivamente, buscamos un método de evaluación que además de fiable, sea aplicable al universo de riesgos de seguridad y medio ambiente. Hay que mencionar que para evaluar riesgos concretos hay multitud de métodos e incluso herramientas informatizadas, y, posiblemente estos alcancen en conjunto un nivel mayor de eficacia que los generalistas, pero repetimos, no son estos nuestro objetivo[10].

Así, de entre los numerosos métodos de evaluación general de riesgos de seguridad se han seleccionado para su análisis, como más representativos el Cuantitativo Mixto, el SEPTRI, y el Método Mösler.

[10] Por este motivo no se han analizado métodos específicos como el HAZOP, para procesos industriales, el Messeri para incendios, el Magerit para información, o los específicos de medio ambiente.

El proceso experimental que vamos a seguir consiste, como se ha enunciado, en aplicar cada uno de estos métodos a un caso tipo, ficticio, que se propone. Se tratará simplemente de observar su comportamiento y analizar los resultados obtenidos, extrayendo finalmente unas conclusiones. La comparación de las conclusiones obtenidas tras al aplicación de las tres metodologías, nos dará pié para aventurar unas conclusiones generales. Evidentemente, esto no puede impedir que se pueda encontrar cualquier otro método no incluido en este experimento y cuyo comportamiento resultase mejor que el obtenido con los tres mencionados. Tras la exposición del método se procederá en cada caso a su aplicación práctica al supuesto teórico que se plantea.

Como contraposición a los métodos mencionados, se efectúa una referencia general a los métodos para evaluación ambiental.

Los parámetros que se van a someter a este análisis experimental, para cada uno de los métodos de evaluación elegidos son:

- Aplicabilidad de cada uno de los métodos de evaluación a los riesgos de seguridad y medio ambiente en toda su extensión.
- Grado de objetividad o subjetividad de las valoraciones de los criterios o factores de cada uno de los métodos.
- Fiabilidad de los resultados obtenidos.
- Alcance del método de evaluación; si permite o no llegar a todos las fases de la gerencia, incluyendo una propuesta de tratamiento de riesgos.
- Si posibilita la representación gráfica; su aptitud como instrumento para elaborar el mapa de riesgos.

3.1. Planteamiento del supuesto al que se le aplicarán los métodos seleccionados

La eficacia de los métodos de evaluación, objeto de este estudio, se va a medir, como ya se ha explicado, aplicando cada uno de estos al caso teórico, que bien pudiera responder a la realidad que se propone. Se ha buscado un supuesto extremadamente sencillo, con determinados riesgos fácilmente perceptibles y graves desde el punto de vista cualitativo. Por otra parte, el catálogo de riesgos identificados se ha reducido hasta el mínimo imprescindible para poder llevar a cabo el estudio.

Se parte de una sencilla identificación de riesgos común para todos los métodos. Con estas premisas, el caso ficticio que se plantea es el siguiente:

"Se trata de un recinto fabril, que alberga maquinaria de valor estimable, y difícil reposición. Consta de una nave con puerta normal de chapa. No dispone de ninguna medida de seguridad. Como medio de protección contra incendios sólo cuenta con extintores. La nave se encuentra en una parcela protegida por una valla de obra muy deteriorada, que no impide el paso. No hay ningún tipo de control de accesos. En la parcela se encuentra un depósito de combustible sin protección ninguna y en el que se aprecia una fuga de combustible. Este recinto se encuentra en un polígono dentro de una zona socialmente conflictiva. En el último año se han producido tres intrusiones en el interior de la fábrica, con robos de objetos varios en dos ocasiones, provocando en una de ellas la parada de la máquina principal por los daños ocasionados. El acceso por ajenos no autorizados a la parcela es muy frecuente."

En el supuesto planteado se identifican los siguientes riesgos:

- *Riesgo de incendio.*
- *Riesgo de robo.*

- *Riesgo de daños.*[11]

- *Riesgo medio ambiental por vertido de combustible.*

Se evaluarán estos riesgos aplicando diferentes métodos.

3.2. Aplicación del Método Cuantitativo Mixto [12]

3.2.1 Descripción del Método

Se trata de un método cuantitativo para identificar y evaluar los riesgos. Consta de las siguientes fases:

- Identificación del riesgo.
- Análisis del riesgo.
- Evaluación del riesgo.
- Cálculo y clasificación del riesgo.

La evaluación se efectúa partiendo de unas variables o criterios, calificándolas y ponderándolas. Se consideran las siguientes variables o criterios, de las que se especifica su posible valoración y clasificación:

- **Criterio de Probabilidad (P**). Número de veces que se manifiesta el riesgo**.**
  Valores desde 0,1 (prácticamente imposible) hasta 10 (Certeza segura).

[11] Se adopta la denominación de "riesgo de daños" con la finalidad de contribuir al estudio, sin tipificar el daño como definición del riesgo. A estos efectos, consideramos "Riesgo de Daños" como el daño ocasionado en al fábrica de nuestro caso, ocasionado sin otra finalidad.

[12] Para la descripción y aplicación del método cuantitativo mixto se ha seguido el contenido del XV Master de Seguros y Gerencia de Riesgos de la Fundación MAPFRE.

- **Criterio de Exposición (E).** Número de veces que se manifiesta el agente que causa el daño y la intensidad. Toma valores desde 0.1 (muy raro, una vez al año) hasta 10 (Continúa o permanente).

- **Criterio de Consecuencia (C).** Cuantificación de los daños si se produjesen.

  Toma valores desde 1 (perceptible, daños superiores a 1.600 $) hasta 100 (catastróficos, daños mayores de 1,5 M $).

CÁLCULO DEL RIESGO:

$$R = P \times E \times C$$

3.2.2. Clasificación del Riesgo

La clasificación del riesgo viene dada por:

- ***Aceptable***: Para R menor o igual a 20.
- ***Posible:*** Para R mayor que 20 y menor o igual que 70.
- ***Considerable***: Para R mayor que 70 y menor o igual que 200.
- ***Alto***: Para R mayor que 200 y menor o igual que 400.
- ***Muy Alto***: Para R mayor que 400 y menor o igual a 10.000.

3.2.3 Resultados de la Evaluación de los Riesgos Identificados en el Caso

A continuación en la *Tabla Núm. 1*, se muestran los resultados obtenidos tras la evaluación de los riesgos identificados, en el caso expuesto anteriormente:

RIESGO	VALOR DE LOS FACTORES			CUANTIFICACIÓN DEL RIESGO R	CLASE DE RIESGO
	PROBABILIDAD (P)	EXTENSIÓN (E)	CONSECUENCIA (C)	R = P x E x C	
Incendio	4	9	50	1.800	Muy Alto
Robo	7	9	25	1.575	Muy Alto
Daños	6	9	35	1.890	Muy Alto
Medio Ambiental	8	10	30	2.400	Muy Alto

3.3.4. Análisis Crítico

A. Aplicabilidad del Método Cuantitativo Mixto.

- No siempre es fácil aplicar las variables debido a su carácter taxativo, por ejemplo la probabilidad pasa de posible o poco probable, a ocurrir la mitad de las veces. En el caso propuesto, es difícil determinar si el riesgo de incendio puede ocurrir la mitad de las veces, o si es posible pero poco probable. Se ha optado por dar un valor intermedio.

- El criterio de exposición no es fácil de aplicar a riesgos como los identificados, ya que la exposición a los mismos será casi siempre permanente. Se mezclan criterios de frecuencia (una vez al día o a la semana) con criterios de permanencia (permanente), lo que dificulta su aplicación a riesgos como el de robo o el de incendio (se puede robar en cualquier momento pero será más probable cuando no haya nadie en la fábrica;

situación que no cuadra ni con una vez al día ni con "permanentemente". Lo mismo sucede con el resto de riesgos identificados.

B. Grado de objetividad del Método Cuantitativo Mixto.

- La aplicación de los criterios es subjetiva, a lo que contribuye lo razonado anteriormente, así, el evaluador decidirá con su exclusivo criterio si opta por un valor u otro o por un intermedio.
- La valoración de los daños tampoco es fácil, se puede razonar que es posible robar todo el continente de la fábrica, pero esta probabilidad en cualquier caso siempre será menor que el hecho de que roben cualquier cosa. Ante esto, ¿cómo se valora el riesgo de robo?
- El mismo razonamiento vale para el riesgo que hemos denominado de daños, sobre el que tampoco se pueden determinar sus consecuencias.
- La clasificación de los riesgos, que establece como única, dependerá de la política de riesgos y circunstancias propias de cada empresa.

C. Fiabilidad de los resultados obtenidos del Método Cuantitativo Mixto.

- En el ejemplo propuesto, para todos los riesgos identificados se obtiene la máxima clasificación "Riesgo muy alto". A nuestro juicio no responde a la realidad. No se trata de riesgos que hagan inviable el negocio si se manifiestan (de hecho ya se han producido robos y daños, serios y preocupantes, pero en modo alguno de gravedad tal que aboquen a la empresa a la desaparición). Posiblemente se hayan obtenido estos resultados debido a la valoración alta de la extensión, lo que lleva a concluir que los riesgos de exposición permanente estarían sobrevalorados; así por ejemplo el riesgo de robo en un establecimiento estará sobrevalorado frente al riesgo de hundimiento de una plataforma en fase de montaje a causa de la diferente exposición.

D. Alcance del método de evaluación Cuantitativo Mixto.

- El criterio para la clasificación del riesgo en función de su valor no tiene por qué ser el mismo para todas las empresas, al afectarlas en grado diferente.
- En el caso del ejemplo, no hay criterios suficientes para decidir si las consecuencias del robo, o del riesgo de daños, son serias, muy serias o desastrosas. En el caso, pese a conocer que se trata de riesgos muy probables y que provocan importantes daños (paralización de la máquina principal) no es posible ajustarse a la clasificación propuesta.
- La amplitud de los intervalos para clasificar los riesgos lleva a que riesgos aparentemente diferentes en gravedad, acaben considerarse iguales con este método. Esta cuestión haría muy difícil aplicar prioridades.
- No establece criterios para el tratamiento de los riesgos.

E. Posibilidad de representación gráfica del Método Cuantitativo Mixto.

- No permite la representación gráfica del riesgo en un eje de abscisas y ordenadas al ser función de tres variables. Precisa una representación tridimensional.

3.3. Aplicación del método SEPTRI[13]

3.3.1 Descripción del Método

A priori se concibe como un método general con validez para todos los riesgos. Sus fases son la evaluación, la comparación, jerarquización de los riesgos y la propuesta de tratamiento. Considera los siguientes criterios o variables:

[13] Para la descripción y aplicación del método SEPTRI se ha seguido el contenido del XV Master de Seguros y Gerencia de Riesgos de la Fundación MAPFRE.

- **Probabilidad (P).** Establece doce gradaciones según el periodo de recurrencia, permitiendo intercalar entre dos valores. Va desde el valor 0,1 para un accidente cada 1.000 años, hasta el valor 10 para más de un accidente al día.
- **Exposición (E)** se gradúa en función de la frecuencia de la operación. Toma valores desde 0,5 para frecuencia de más de 100 años, hasta 10 para frecuencia continúa.
- **Intensidad (I)**. Se define como la media aritmética de la **Intensidad Máxima.**

I = (Intensidad Máxima Expuesta (Ir) + Intensidad Máxima Probable (Ip))/ 2

I = (Ir + Ip) / 2.

3.3.2 Clasificación del Riesgo

El valor de la Intensidad Máxima Expuesta (Ir), **dependerá del** Valor Máximo Expuesto (VME) **o de la** Pérdida Máxima Posible (PMP) **tomando valores desde 1 para VME de 100 ó PMP de 0,05 %, hasta 10 para VME mayor que el patrimonio de la empresa o PMP del 100%.**

- El valor de la **Intensidad Máxima Probable (Ip)** dependerá de la **Pérdida Máxima Probable (PMPr)** tomando valores desde 1 para PMPr de menos de 50 o del 0,01 %, hasta 10 para PMPr de más de 50 millones ó mayor del 40 %.
- **Nivel de Seguridad (S)** este coeficiente se calcula como la suma de coeficientes parciales, según cuente o no con medidas o sistemas de seguridad. No puede ser menor que 1.

- **Cálculo del Riesgo (R)** El riesgo se calcula en función de los parámetros expuestos, de acuerdo con la siguiente fórmula:

CÁLCULO DEL RIESGO:

R = (P x E x I) / S

Sustituyendo I por (Ir + Ip)/ 2:

R = (P x Ex ((Ir + Ip) /2)) / S

El método SEPTRI finaliza con una propuesta de tratamiento en función del valor del riesgo obtenido en la evaluación.

3.3.3 Resultados de la Evaluación de los Riesgos Identificados en el Caso

A continuación en la *Tabla N. 2*, se muestran los resultados obtenidos de la evaluación de los riesgos identificados, en el caso expuesto anteriormente:

RIESGO	VALOR DE LOS FACTORES						CUANTIFICACIÓN DEL RIESGO R	CLASE DE RIESGO
	PROBABILIDAD (P)	INTENSIDAD I= (Ir+Ip)/2			EXTENSIÓN (E)	NIVEL SEGURIDAD S		
		Ir	Ip	I			R= (P x I x E) /S	
Incendio	3 (26-25 años)	8	7	7,5	9	2	101,25	Grave
Robo	7 (31-365 días)	6	3	4,5	9	2	141,75	Grave
Daños	7 (31-365 días)	6	3	4,5	9	2	141,75	Grave
Medio Ambiental	10 (menos de un día	5	5	5	8	2	200	Extremo

3.3.3 Análisis Crítico

A. Aplicabilidad del método.

- El concepto de frecuencia de operación no es directamente aplicable a los riesgos que no están sujetos a ninguna operación, salvo que se tomen como continuos lo que introduce distorsiones.
- El criterio de probabilidad, al remitir a la frecuencia de los accidentes ocurridos, no se puede aplicar a riesgos como los identificados, probables pero sin que hayan llegado a manifestarse, por ejemplo el incendio. Tampoco se puede aplicar a riesgos continuos como la fuga de combustible. Para estos casos si se pretende aplicar el método SEPTRI, se cae en un gran subjetivismo, forzando un valor sin criterio alguno.

  En el caso propuesto, se ha optado por valorarlo de algún modo con el fin de continuar el análisis del método.
- Los conceptos de PMP, VMP, etc., son propios del riesgo de incendio, pero su aplicabilidad a otros riesgos no resulta tan clara en tanto en cuanto no se va a producir una destrucción por proximidad.
- La extensión, como frecuencia de la operación no es aplicable a riesgos que no están sujetos a operaciones.

B. Grado de objetividad.

- Las dificultades para aplicar los criterios expuestos, lleva a introducir el criterio del evaluador para valorarlos, con lo que se pierde la objetividad.

C. Fiabilidad de los resultados obtenidos.

- Los criterios para asignar valores al coeficiente por nivel de seguridad no reflejan la realidad de la seguridad en una instalación, dando excesiva importancia a aspectos teóricos y administrativos, como por ejemplo si cuenta con política de seguridad, con

programa de gerencia de riesgos, con programa de control de calidad, si tiene integrada la prevención en el diseño y si ha sido auditado, factores que en conjunto tienen más peso que si se cuenta o no con medidas de seguridad.

D. Alcance del método de evaluación.

- Como punto favorable, este método es el único de los analizados que incluye propuestas de tratamiento.

E. Posibilidad de representación gráfica.

- No permite la representación del riesgo el un eje de coordenadas, al definirse por cuatro factores, por lo que no es apto para elaborar un mapa de riesgos.

3.4. Análisis del método Mösler para seguridad [14]

3.4.1 Descripción del Método

Se trata de uno de los métodos de evaluación más utilizados en el ámbito de seguridad patrimonial. Aparentemente se trata de un método cuantitativo con base científica que, según algunas definiciones, combina métodos probabilísticos con estadísticos a través de esquemas matriciales.

El Método Mösler se desarrolla en cuatro fases concatenadas:

- ***Fase 1:*** *Identificación de riesgos.*
- ***Fase 2:*** *Análisis de riesgo.*

Se utilizan para este análisis una serie de coeficientes (criterios):

[14] Para la descripción y aplicación del método MOSLER se ha seguido el contenido "Manual para el Director de Seguridad", de Gómez Merelo, editado por E.T. Estudios Técnicos S.A. 1ª Edición. 1996

- **Criterio de Función (F):** Mide cuál es la consecuencia negativa o daño que pueda alterar la actividad y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde "Muy levemente grave" a "Muy grave.
- **Criterio de Sustitución (S):** Mide con qué facilidad pueden reponerse los bienes en caso que se produzcan alguno de los riesgos y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde "Muy fácilmente" a "Muy difícilmente".
- **Criterio de Profundidad o Perturbación (P):** Mide la perturbación y efectos psicológicos en función que alguno de los riesgos se haga presente (Mide la imagen de la firma) y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde "Muy leves" a "Muy graves".
- **Criterio de extensión (E):** Mide el alcance de los daños, en caso de que se produzca un riesgo a nivel geográfico y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde "Individual" a "Internacional".
- **Criterio de agresión (A):** Mide la probabilidad de que el riesgo se manifieste y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde "Muy reducida" a "Muy elevada".
- **Criterio de vulnerabilidad (V):** Mide y analiza la posibilidad de que, dado el riesgo, efectivamente tenga un daño y cuya consecuencia tiene un puntaje asociado, del 1 al 5, que va desde "Muy baja" a "Muy Alta".

- ***Fase 3:*** **Evaluación del riesgo.**

  Esta fase tiene por objeto cuantificar el riesgo previamente definido y analizado, se consideran los siguientes aspectos:

  - **Cálculo del carácter del riesgo. (C).** Se obtiene sumando la importancia del riesgo (I) a los daños ocasionados (D).

Cálculo del carácter del riesgo

C = I + D

A su vez estos conceptos de los que parte se definen:

- Importancia del Riesgo (I), como producto del criterio de función (F) por el de sustitución (S). (I = F x S).
- Daño (D), como resultado de multiplicar el criterio de profundidad (P) por el de extensión (E). Así D = P x E
- De lo anterior, el carácter del riesgo (C) se calcula: C = I + D = (F x S) + (P x E).

o **Cálculo de la probabilidad. (P)** como producto del criterio de agresión (A) por el de vulnerabilidad (V). Así:

Cálculo de la probabilidad

P = A x V

o **Cuantificación del riesgo considerado (ER).** Resultante del producto del cálculo del carácter del riesgo (C) por la probabilidad (P).

Cálculo del riesgo considerado

ER = C x P,

sustituyendo:

ER= (I + D) x P = ((F x S) + (P x E)) x (A x V)

- **Fase 4: Cálculo y clasificación del riesgo.** Esta fase tiene por objeto clasificar el riesgo de acuerdo con su valor obtenido, aplicando la siguiente tabulación, recogida en la *Tabla N. 3* :

VALOR	RIESGO
2 y 250	Bajo
251 y 500	Pequeño
501 y 750	Normal
751 y 1000	Grande
1001 y 1250	Riesgo Elevado

3.4.2 Resultados de la Evaluación de los Riesgos Identificados en el Caso por el Método Mösler

Tabla N. 4

RIESGO	VALOR DE LOS CRITERIOS						Cuantificación Del riesgo (ER) (F x S) + (P x E)) x x (A x V)	Clase de riesgo
	F	S	P	E	A	V		
Incendio	Gravmte 4	MD 5	MGrv 5	Reg 3	Elevad 4	MuyElv 5	700	Normal
Robo	Gravmte 4	SD 3	Limit 3	Local 2	MuyElv 5	MuyElv 5	450	Reducido
Daños	Gravmte 4	SD 3	Grv 4	Local 2	MuyElv 5	MuyElv 5	500	Reducido
Medio Ambiental	Gravmte 4	No aplica	Grv 4	Reg 3	MuyElv 5	Elevad 4	400	Reducido

3.4.3 Análisis Crítico

A. Aplicabilidad del método.

- Al partir de criterios tasados y cerrados, no permite aplicar otros criterios que a juicio del evaluador pudiesen ser relevantes.
- Desde otro punto de vista, se viene obligado a utilizar todos los criterios, de lo contrario no es viable el método. Pero puede suceder que no sea posible aplicar algún criterio.
- En nuestro ejemplo no se aplica el criterio de sustitución al daño medio ambiental provocado por la fuga de combustible, y con reservas se ha aplicado el criterio de extensión (¿Cómo se aplica si se trata de una empresa con un solo establecimiento?).

B. Grado de objetividad.

- Pese a su pretendida objetividad y carácter científico, la aplicación de los criterios es totalmente subjetiva, lo que llevará indefectiblemente, a resultados subjetivos.

C. Fiabilidad de los resultados obtenidos

- Un aspecto negativo es, a nuestro juicio, la gran amplitud de los intervalos para clasificar el riesgo. Esto lleva a que no se afine en la comparativa de los riesgos, factor clave para establecer prioridades.
- Por otra parte, pese a tratarse de riesgos ciertamente relevantes, a partir del caso de referencia, se observa que los resultados que arroja este método son reducidos para el robo (pese a la gran probabilidad de robo, a que ya ha sucedido varias veces ya que han sustraído objetos de cierto valor), reducidos para daños (sobre los que pesa la misma motivación expuesta para el robo, con el agravante de que los daños ya ocasionados han llegado a provocar la parada de la máquina principal), el riesgo medioambiental, pese que se trata casi de un riesgo cierto (se aprecia una fuga de combustible) también se clasifica como reducido.

En la misma línea, el riesgo de incendio se valora como normal, tratándose de un recinto con evidente carga de fuego y con protección deficiente y considerando la pérdida de toda la fábrica si se producía un incendio.

D. Alcance del método de evaluación.

- La gradación del riesgo que se propone no responde a ningún criterio ni se establecen qué consecuencias tiene el que un riesgo sea reducido, normal o elevado.
- No se proponen priorizaciones para los posibles tratamientos.

E. Posibilidad de representación gráfica.

- Como aspecto favorable se considera que permite cierta cuantificación y presentación de resultados, al reducirse todos los factores a probabilidad y consecuencia.
- También se considera favorable el hecho de que se base en más factores que otros métodos también cerrados en cuanto a criterios de valoración.

3.5. Conclusiones de los métodos analizados

Como conclusiones generales a los tres métodos de evaluación analizados se pueden mencionar las siguientes:

- No se trata de métodos que puedan aplicarse a todos los riesgos ni a todas las situaciones. Al partir de unos criterios taxativos, condiciona su aplicabilidad al universo de riesgos y de circunstancias; en el caso propuesto, en más de una ocasión no se han podido aplicar, determinados criterios de un método.
- Esta falta de adecuación a la realidad distorsiona los resultados. Por una parte el empeño en aplicarlos conlleva la introducción de la carga subjetiva, por otra los resultados obtenidos van a carecer de la fiabilidad necesaria.

- La falta de fiabilidad de los resultados se pone de manifiesto por una parte, al obtener el mismo resultado de riesgo en cada método, para los cuatro identificados. Arrojando por otra parte, grandes diferencias entre los obtenidos por uno u otro método; así van desde el resultado de riesgo reducido para todos los identificados obtenido por el Mosler (pese a que se tratan de riesgos cualitativamente graves) a catastróficos, muy alto grave, según los otros dos métodos.
- En general no contemplan la evaluación en todo a su extensión, así no suelen incluir el tratamiento de riesgos.
- Establecen clasificaciones de riesgos cerradas y supuestamente universales para todas las organizaciones, cuando será cada empresa u organización la que deba determinar, a la vista del valor del riesgo y sus consecuencias, si para ellos es tolerable, intolerable, catastrófico, etc.
- La representación de los riesgos en un eje de coordenadas, en función de la valoración obtenida con estos métodos, sólo es posible con el Mösler.

3.6. Referencia a métodos para valoración del riesgo medioambiental

Las evaluaciones específicas de riesgos ambientales siguen parámetros diferentes al resto de evaluaciones, toda vez que en muchos casos se basa en proyecciones a largo y muy largo plazo sobre las posibles consecuencias. Debiendo considerar por otra parte múltiples factores como receptores del posible daño, factores incluso ajenos a la instalación.

Tras una identificación y primera valoración del riesgo, incluso por métodos cualitativos, se procede a aplicar el método de evaluación específico para el riesgo detectado.

Se aplicarán métodos matemáticos que posibiliten la proyección temporal del riesgo y sus consecuencias hacia diferentes sujetos pasivos receptores del daño. Con este fin se efectúan

simulaciones matemáticas, introduciendo escenarios variables y evaluando las consecuencias para cada caso.

En este contexto, los métodos de evaluación objeto de este estudio, pueden jugar un importante papel en las evoluciones ambientales, como primeros evaluadores del riesgo. Por este motivo será importante disponer de un método que permita el acercamiento rápido al problema ambiental y una primera evaluación que será tanto mejor en función de su alejamiento de vicios como el excesivo subjetivismo, su imposible aplicabilidad, o su escasa fiabilidad de los resultados.

Aplicando este criterio al caso ficticio propuesto, el evaluador identificaría, analizaría y efectuaría una primera evaluación, cuantificando el riesgo que puede suponer para el medio ambiente un depósito de combustible en medio de una parcela prácticamente abierta y del que se está saliendo el combustible.

También podría llegar a efectuar, en la medida de sus posibilidades, la identificación de posibles receptores del daño, así si en el entorno hay cauces de ríos, especies protegidas, vegetación, etc.

Para lo anterior es indispensable contar con un buen check list de contenido ambiental, cuya aplicación no precise expertos.

Estos datos se les pasarían a los expertos medio ambientales para que aplicasen el método de evaluación correcto. Siguiendo con el caso propuesto, mediante las evaluaciones específicas se determinaría el grado de afectación presente y futuro del ecosistema dañado por el escape de combustible. Si se ha producido la filtración, si ha contaminado cauces, etc.

Referencia a la Ley de Responsabilidad Medioambiental.

El panorama de la Evaluación Medioambiental se ha visto alterado tras la Ley 26/2007, de 23 de octubre, de Responsabilidad Medioambiental sobre cuya finalidad cabe mencionar que es

prevenir, evitar y reparar el daño medioambiental. Se trata de devolver los recursos naturales a su estado original. No se trata por tanto de una norma para asegurar la responsabilidad derivada del daño medioambiental.

Las empresas con potencial riesgo medioambiental, recogidas en la propia normativa, vienen obligadas a constituir una garantía financiera para asegurar que dispondrán de los recursos necesarios con los que hacer frente a sus obligaciones de prevenir el daño, evitarlo o repararlo. La garantía financiera puede ser un aval bancario, una póliza de seguro o una reserva técnica.

3.7. Referencia a métodos generales para evaluación del riesgo operacional.

Acorde con la importancia del Riesgo Operacional, de lo que ha quedado constancia en este texto, la evaluación de los mismos, como fase crucial para su gestión, ha sido y es objeto de numerosos trabajos, encaminados generalmente al estudio y obtención de métodos adecuados. Efectivamente, si indagamos mínimamente en este ámbito podemos encontrar sin problemas variada literatura al respecto y, de igual modo, prolifera la oferta de cursos para "evaluar el riesgo operacional". Otro tanto podemos decir de los sistemas de gestión del Riesgo Operacional comercializados. Incluso desde las normativas sectoriales, *BASILEA y SOLVENCIA*, se proponen métodos para valuar el riesgo operacional.

Como consecuencia, desde el ámbito empresarial llevan ya tiempo aplicándose un variado elenco de estos métodos de evaluación.

Podemos preguntarnos el porqué del presente trabajo proponiendo nuevos métodos para evaluar también riesgos operacionales, (ya ha quedado suficientemente razonado que los de seguridad y medio ambiente son riesgos operacionales). El lector que haya seguido esta obra hasta este punto tendrá gran parte de la respuesta a este posible interrogante. Las peculiaridades de los riesgos de seguridad y por ende de su propia gestión hacen a esta

disciplina acreedora de un tratamiento especial dentro del conjunto de la gerencia de riesgos en general y de los operacionales en particular. Y esto se corrobora además, si se considera la escasez de estudios que traten la seguridad desde una óptica gerencial.

Con la evaluación misma sucede otro tanto, la especificidad de los riesgos obliga a tratamientos especializados.

Pero más allá de este necesidad de tratamiento especializado, siguiendo el camino analítico con marcada vocación experimental por el que pretende discurrir el presente trabajo, no podemos dejar de ver con cierto detalle la situación de los métodos para evaluar el riesgo operacional, sin que esto implique, como en el caso de los análisis empíricos de algunos de los métodos de evaluación de seguridad que se ha efectuado, que nuestro objetivo sea analizar un sinfín de estos métodos.

Pero llama la atención que estos métodos de evaluación, casi de forma general, ponen de manifiesto la dificultad, cuando no imposibilidad, de cuantificar el riesgo operacional. Así es muy normal que se basen en valoraciones subjetivas y, frecuentemente, en autoevaluaciones de los propios interesados. Lo que presenta evidentes problemas a la hora de comparar resultados y dificultan, cuando no resulta imposible, que se pueda tener una idea clara y precisa del nivel de riesgo.

Efectivamente, partiendo de la gran dificultad para cuantificar estos riesgos, incluyendo los de seguridad y los de medio ambiente, si al menos existiese algún parámetro o "regla para medir el riesgo" o patrón admitido por las organizaciones, de manera más o menos generalizada como para constituir la referencia de las mediciones, podría paliarse un tanto este inconveniente. Persistiría no obstante la necesidad de ajustar también los criterios que llevan a la apreciación del nivel de riesgo, las evidencias del riesgo. Pero la realidad es que en la actualidad no se cuenta con esta unificación de criterios, por lo que desde nuestra humilde opinión, los resultados devienen poco significativos.

En estos métodos hemos encontrado, con bastante frecuencia, que formulan muchas cuestiones desde una óptica general, lo que no llevará nunca a la realidad del riesgo. Nos referimos a cuestiones tan generales como "Existe riesgo de incendio" o "Es posible que se produzca un robo", contestar a este tipo de cuestiones desde un conocimiento no superficial de estos riesgos, exige a su vez aplicar una metodología concreta. El problema se agrava si, como se expuso, el propio método no incluye la definición de una matriz para parametrizar los factores por los que pregunta, mediante la que el evaluador que responde a las cuestiones, no tenga dudas sobre el alcance de una probabilidad o una importancia media, baja o alta, por ejemplo.

Es más, si se analizan desde esta perspectiva los denominados métodos para medir el riesgo operacional establecidos desde la mencionada normativa sectorial, referencia obligada para la gestión de riesgos de las empresas, se aprecia que en los mismos no se incluyen parámetros que permitan llegar a la cuantificación del riesgos, se tratan de sistemas para, desde su relación con el riesgo cuantificar los capitales necesarios. Efectivamente, se propugnan tres métodos, el básico simplemente consiste en asumir que el capital para cubrir estos riesgos es un porcentaje de los ingresos de la empresa, lo que obviamente no es ninguna evaluación de riesgos.

El estándar también lleva al cálculo del capital necesario partiendo de los ingresos por líneas de negocio aplicándoles unos porcentajes.

Mientras que los métodos avanzados, será la organización que se acoja a este sistema la que los desarrollará, debiendo necesariamente incluir para incluir requisitos cualitativos y cuantitativos. Pero tampoco entre estos últimos se llega a definir parámetros para medir las evidencias, que permitan comparar los niveles de riesgo, marcando de forma general qué aspectos deben recogerse en estos métodos y hasta qué nivel de riesgos deben alcanzar. Pero no se llega en ningún caso a definir cómo se mide el nivel de riesgo.

Estos problemas nos llevaron a buscar algún método mediante el que se pudiera llegar a medir las evidencias de riesgo. Contando con que siempre habrá una apreciación subjetiva por medio, en nuestras propuestos trataremos de acotarla reduciéndola todo lo posible.

Adelantándonos al contendido de los siguientes capítulos, apuntamos ya que, desde nuestro punto de vista, para reducir la subjetividad de los métodos de evaluación, debe partirse de la definición clara de los parámetros que van a considerarse, de forma que lleguen de verdad al riesgo, sin caer en generalidades. Para ello un buen sistema será integrar las evidencias o factores de riesgo. Luego habrá que parametrizarlos, para lo cual en la medida en que se contase con patrones admitidos por la comunidad de gerencia, se llegaría a valoraciones, que además de objetiva, permitirían la comparación entre los niveles de exposición al riesgo de las organizaciones. Pero si, como ocurre actualmente, no se cuenta con esos patrones, la opción más coherente es definir metodologías lo suficientemente explícitas y detalladas para que los interesados que deban conocer el nivel de riesgo, tengan una auténtica noción del mismo.

3.8. Aplicación de los métodos de evaluación estudiados para elaborar los mapas de riesgo

A partir de la evaluación se podrá determinar el mapa de riesgos, que no es más que la representación gráfica de los riesgos en un eje de coordenadas.

Esta representación va a permitir establecer prioridades de actuación en función del posicionamiento de los riesgos en la tabla.

Se considera un método muy útil para las presentaciones de riesgos a la Dirección, o al escalón jerárquico más alto de la organización, por su rápida visualización y carácter intuitivo.

Lógicamente, la representación del riesgo en un eje de abscisas y ordenadas precisa que la función definitoria del mismo se componga de dos parámetros.

Considerar la expresión del riesgo como función de tres parámetros obligaría a una representación tridimensional o a buscar otro tipo de relación matemática, tal y como establece la evaluación medio ambiental mediante *ecuaciones Probit*.

Las empresas adoptan diversos programas para confeccionar sus mapas de riesgo, generalmente parten de la expresión matemática del riesgo como función de la probabilidad y la intensidad, la consecuencia o la importancia[15].

Para estos métodos, a partir del mapa, el tratamiento de riesgos vendrá condicionado en función de la posición que ocupe en la tabla: en la parte superior los más importantes y en la de la derecha los de mayor probabilidad. Los más graves por intensidad y probabilidad serán los de la parte superior derecha, que coincide con los que precisa un tratamiento más urgente.

El problema de esta representación es que la actuación no viene condicionada de forma directa por la magnitud del riesgo, si no por su probabilidad o por su intensidad. Así dos riesgos de igual valor podrán no ser objeto de la misma prioridad en función de si ese valor se obtiene por una alta probabilidad o una alta intensidad o un valor intermedio para ambas[16].

Este sistema no permite la inclusión de un tercer parámetro para la valoración del riesgo. Por este motivo, como ya hemos visto, no son aptos para este tipo de representaciones gráficas los métodos como el Cuantitativo Mixto o el SEPTRI.

Otros sistemas de mapa de riesgos como el utilizado por algunas grandes empresas, solucionan este problema e incluyen un tercer parámetro para el cálculo de riesgos, mediante un factor diferenciador como es el diferente grosor del punto. Así el riesgo es función además de la probabilidad y de la intensidad, de las medias de control con que cuenta. A la representación

[15] La relación matemática del riesgo, como función de la probabilidad y la intensidad, es expresada por algunos autores sustituyendo la probabilidad por la frecuencia y/o la intensidad por la consecuencia.

[16] Diferentes valores para probabilidad e intensidad llevarán a una posición diferente en la tabla, incluso para valores totales de riesgos iguales.

tipo descrita, le añaden el tamaño del punto. Ciertamente le son aplicables los inconvenientes anteriormente reseñados.

A continuación se inserta un ejemplo gráfico de mapa de riesgos.

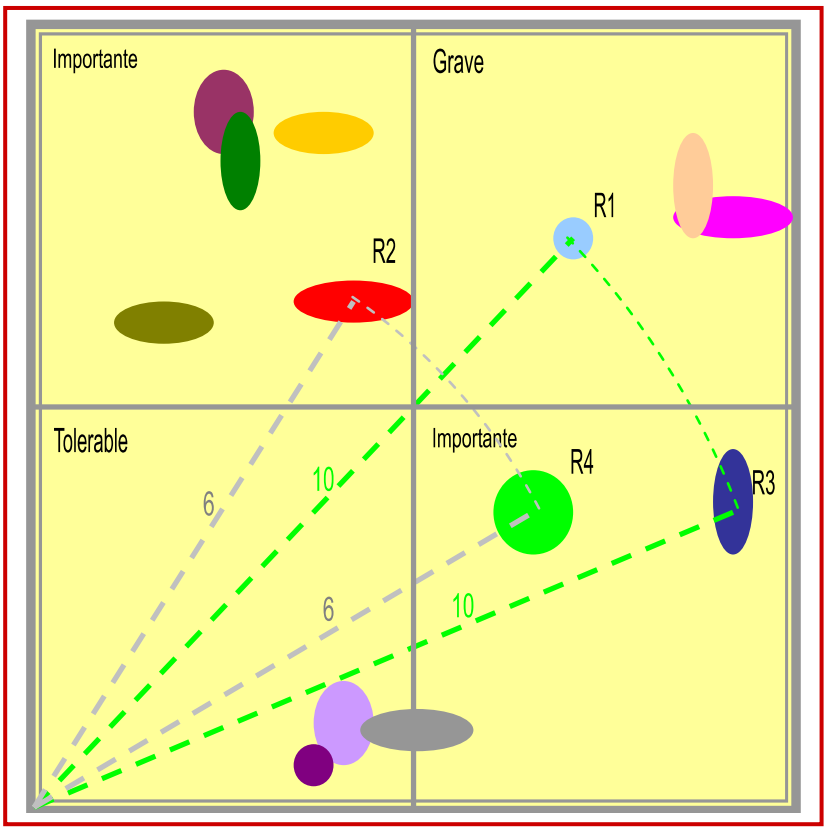


Fig. 6. Mapa de Riesgos por aplicación de métodos generales para evaluar el riesgo operacional. Fuente: Elaboración Propia

Como se puede apreciar, pese a tratarse de riesgos de igual valor (R1 con R3 y R2 con R4), en virtud de su posición en uno u otro cuadrante, se les consideraría diferentes.

La diferente forma y tamaño de los puntos indica la consideración gráfica de otros factores (si se cuenta con medidas para controlarlo, por ejemplo).

CAPÍTULO 4: APROXIMACIÓN CONCEPTUAL AL RIESGO

4.1. Formulación del riesgo en función de la probabilidad y de la intensidad, daño o consecuencia. Su concepción como esperanza matemática.

Está comúnmente admitido que el riesgo es función de la probabilidad y de su consecuencia, así la ***Guía ISO/ CEI 73*** lo define como la "*Combinación de la probabilidad de un suceso y de su consecuencia"*.

Analizando las posibles funciones matemáticas para calcularlo, como se ha recogido en el Capítulo dedicado al análisis de metodologías de evaluación, no todas responden a una relación de estos dos factores.

Efectivamente, el Método SEPTRI utiliza una función que relaciona la probabilidad, la exposición y la intensidad, ponderándolo todo con la existencia de medidas de seguridad. El Cuantitativo Mixto calcula el riesgo a partir de la probabilidad, de la exposición y de la consecuencia. Y el Método Mösler utiliza la combinación de sumandos y productos de seis factores, partiendo del carácter del riesgo y de la probabilidad. Por otra parte, los métodos utilizados para la evaluación del riesgo operacional, tampoco se circunscriben en su totalidad a la mera combinación de la probabilidad y la intensidad o la consecuencia.

Si bien es cierto que muchos de los parámetros utilizados por estos métodos, pueden subsumirse en un concepto probabilístico, no es menos cierto que no hemos encontrado la fundamentación matemática que lleve a la adopción de estas formulaciones. Hecho que lleva a pensar que esas formulaciones pretenden responder más a criterios prácticos que a fundamentos científicos.

El concepto matemático más generalizado definir el riesgo, lo concibe como *la esperanza matemática de la consecuencia de un suceso indeseable*. Lo que lleva al producto de la probabilidad por la consecuencia.

El riesgo es una medida del peligro que los sucesos indeseables representan para los valores humanos, ambientales o económicos. Se expresa normalmente mediante la probabilidad de que acontezcan sucesos indeseables junto con las consecuencias que éstos implicarían. Como hemos recogido, se estima a menudo mediante la esperanza matemática de las consecuencias de un suceso indeseable; concepto que desemboca en el producto "probabilidad x consecuencias". Sin embargo, una interpretación más general del riesgo trabaja con la probabilidad y las consecuencias de una manera distinta.

Desde una concepción más enfocada al aseguramiento y a los entornos financieros, también partiendo del concepto de esperanza matemática, se define el riesgo como "la esperanza matemática de las pérdidas posibles".

Estamos tratando de evaluar riesgos de seguridad y medio ambiente, así, cabe preguntarnos si el concepto de esperanza matemática para definir el riesgo, es aplicable también a este tipo de riesgos.

Fijemos pues nuestra atención en el concepto mismo de *esperanza matemática*, que define la Estadística como el *número que formaliza la idea del valor medio de un fenómeno aleatorio*. Es sinónimo del valor medio o esperado.

Cuando la variable aleatoria es discreta[17], la esperanza es igual a la suma de la probabilidad de cada posible suceso aleatorio multiplicado por el valor de dicho suceso. Por lo tanto, representa la cantidad media que se "espera" como resultado de un experimento aleatorio cuando la probabilidad de cada suceso se mantiene constante y el experimento se repite un elevado

[17] Es obvio mencionar que una variable aleatoria discreta es la que sólo puede tomar valores definidos, por ejemplo la puntuación de las caras de un dado.

número de veces. Coincide con la media aritmética cuando todos los sucesos tienen la misma probabilidad, y no siempre este valor que se espera coincidirá con un valor real.[18]

Así, para una variable aleatoria discreta con valores posibles $x_1, x_2 \ldots x_n$ y sus probabilidades representadas por la función de probabilidad $p(x_i)$ la esperanza se calcula como:

$$E[X] = x_1 p(X = x_1) + \ldots + x_n p(X = x_n) = E[X] = \sum_{i=1}^{n} x_i p(x_i)$$

Cuando la variable aleatoria es continua[19], la esperanza se calcula mediante la integral de todos los valores y la función de densidad $f(x)$:

$$E[X] = \int_{-\infty}^{\infty} x f(x) dx$$

Como se observa, el concepto de riesgo como esperanza matemática es útil si se considera un espectro de consecuencias, conociendo la probabilidad de cada magnitud. Por este motivo se utiliza para definir el "Riesgo de pérdidas probables", parámetro esencial en técnica actuarial y financiera.

Ahora bien, ¿cómo podemos aplicar el concepto de esperanza matemática o valor esperado a sucesos que nunca han ocurrido o a sucesos sobre los que no se dispone de estadística alguna? Por ejemplo, un sabotaje puede no haber ocurrido nunca, pero el análisis de los factores y vulnerabilidades puede determinar que es posible, sin que pueda asignársele un valor a la probabilidad de que suceda. Pero es que el concepto mismo de "valor esperado" o "valor medio" se nos antoja de difícil aplicación para definir cualquiera de los riesgos de seguridad y medio ambiente, ¿cómo podemos, por ejemplo relacionar una valoración media con un posible incendio…. O con un posible robo…? Podremos valorar la media de pérdidas ocasionadas por

[18] Por ejemplo, el valor esperado cuando tiramos un dado equilibrado de 6 caras es 3,5. Valor que no coincide con la puntuación de ninguna de las caras, pero es el obtenido del sumatorio de la probabilidad de que salga cada una de las seis caras multiplicada por su valor.

[19] La variable aleatoria continua puede adoptar infinitos valores dentro del intervalo considerado, por ejemplo la talla de los individuos de un grupo.

los incendios o por lo robos. Dato de dudosa utilidad en tanto en cuanto no sea obtenido para el universo de sucesos en el que nos movemos.

4.2 Sobre la probabilidad de que se manifieste un riesgo de seguridad o de medio ambiente.

Parece claro que la estimación del riesgo pasa por "averiguar" la probabilidad de que se manifieste o suceda. Si logramos obtener valores de probabilidad, daremos un gran paso para llegar a la valoración del riesgo, sin desdeñar la necesidad de valorar también las consecuencias o el daño que pueda causar.

Pero esto no es nada fácil como ya se ha ido apuntando. En este apartado pretendemos dar alguna luz que nos ponga en el camino del cálculo de la probabilidad de que sucedan riesgos de seguridad y medio ambiente. Conclusiones que serán de aplicación a gran parte del elenco de riesgos operacionales.

4.2.1. ¿Probabilidad o posibilidad del riesgo?

Indistintamente se utilizan las expresiones "este riesgo es probable" o "este riesgo es posible". Vamos a ver brevemente qué significa cada cosa, y si son o no correctas estas expresiones cuando nos referimos a la posible o probable manifestación de un riesgo.

Posibilidad se define en el RAE como la *"aptitud, potencia u ocasión para ser o existir algo y la aptitud o facultad para hacer o no hacer algo*".

Mientras que, si nos fijamos en la definición de ***probabilidad,*** observamos que introduce cierto criterio de certeza, "*verosimilitud o fundada apariencia de verdad"*. Definición que ya nos

arroja alguna luz; pero más interesante es la ***definición matemática de probabilidad***: *"En un proceso aleatorio, razón entre el número de casos favorables y el número de casos posibles"*[20]. Acepciones que aclaran bastante el concepto, permitiendo concluir que un suceso será posible en la medida en que se aprecie facultad o potencia para que sea o exista, es decir, para que se manifieste.

Como **definiciones más científicas de probabilidad** podemos traer que:

"*La probabilidad de ocurrencia de un determinado suceso podría definirse como la proporción de veces que ocurriría dicho suceso si se repitiese un experimento o una observación en un número grande de ocasiones bajo condiciones similares. Por definición, entonces, la probabilidad se mide por un número entre cero y uno: si un suceso no ocurre nunca, su probabilidad asociada es cero, mientras que si ocurriese siempre su probabilidad sería igual a uno. Así, las probabilidades suelen venir expresadas como decimales, fracciones o porcentajes"* [21].

Como descripción más formal desde el punto teórico, tenemos la que permite definir el concepto de probabilidad mediante la verificación de ciertos axiomas a partir de los que se deducen todas las demás propiedades del cálculo de probabilidades. Así, para determinados contextos, se ha defendido una interpretación más amplia del concepto de probabilidad que incluye las que podemos denominar ***probabilidades subjetivas o personales***, mediante las cuales se expresa el grado de confianza o experiencia en una proposición. Esta definición

[20] Por aplicación de la Regla de Laplace
[21] Definición de probabilidad conocida como definición frecuentista.

constituye la base de los llamados métodos bayesianos, que se presentan como alternativa a la estadística tradicional centrada en el contraste de hipótesis[22].

Queda claro, que si se hace referencia a un valor cuantificado de probabilidad tenemos que estar en condiciones de medirla. Pero para efectuar una medición es imprescindible disponer de una referencia, esa "regla para medir" o "patrón" que venimos echando en falta.

Podemos tener el convencimiento de que un suceso es posible, pero en tanto en cuanto no seamos capaces de medir la probabilidad, conceptualmente no podremos aventurar nada acerca de su probabilidad; si se dice que es probable hay que decir en qué medida y respecto a qué.

Situémonos ante el riesgo de robo en una determinada instalación: observamos el entorno, las medidas, los activos, etc.; el sentido común (junto a la experiencia) nos dirá que es posible que se lleve a cabo, e incluso estaremos en condiciones de matizar aún más y percibir el grado de esa posibilidad.

Ahora, ¿tendríamos elementos de juicio para valorar la probabilidad de que sucediera? No tenemos casos posibles ni favorables, no existen esas referencias, lo que lleva a la imposibilidad de calcular una probabilidad matemática.

No obstante, partiendo de que razonadamente lo estimamos más o menos posible, llegamos a la conclusión de que es más o menos probable.

Estamos ante una probabilidad subjetiva, que se aproximará más o menos a la realidad en la medida en que la basemos en más o menos evidencias.

¿Qué son las evidencias? Son todas las indicaciones e indicios que nos llevan a presuponer la posibilidad de un riesgo; entre éstas incluiríamos los factores de riesgo, las vulnerabilidades, las amenazas, etc. Continuando con el ejemplo del robo, como evidencias que nos hacen

[22] Ver la referencia en este mismo Capítulo a la posible aplicación de los métodos bayesianos para el cálculo de la probabilidad de los riesgos de seguridad y medio ambiente.

pensar en que se incrementa el riesgo de robo, partiendo del incremento de la probabilidad, podemos encontrar apreciaciones tales como que la puerta es fácilmente vulnerable, o que el activo a proteger es muy atractivo para los ladrones, que no se realiza un control de accesos, que no se dispone de ninguna medida de seguridad, e incluso podremos fijarnos en el entorno social y en la existencia o no de robos anteriores o en la zona.

Se podrá también clasificar la probabilidad. Lo que no equivale a su cálculo, sino al establecimiento de un patrón con el que comparar cada situación. Cuántos más parámetros se utilicen para llevar a cabo esta clasificación y cuanto más definidos estén, más nos aproximaremos a la probabilidad real.

Por este motivo, desdeñamos los métodos que no parametrizan adecuadamente la probabilidad; así los que se limitan a mencionar que puede incluirse en determinadas categorías (probabilidad baja, media o alta por lo general) limitándose a dar de pasada unas pinceladas para incluirla enana u otra categoría.

Otro error apreciado en varios métodos es confundir probabilidad con frecuencia. No es necesario mencionar que la frecuencia es simplemente el número de veces que ha sucedido, lo que no puede utilizarse como sinónimo de probabilidad. Sí es factible que como indicio o factor de riesgo se considere la frecuencia; e incluso que, mediando la correspondiente justificación metodológica, se haga depender la estimación subjetiva de la probabilidad con la frecuencia en que ha sucedido, como único parámetro (opción que a nuestro juicio no dejaría de constituir un error, considerando que utilizar sólo un tipo de indicios para apreciarla no constituye un argumento suficientemente potente).

No podemos perder de vista, por otra parte, que para calcular el riesgo, sea cuál sea la fórmula que utilicemos, debe obtenerse una valoración cuantitativa previa de la probabilidad (aún subjetiva) y del daño o las consecuencias.

A continuación, vamos a ver si es posible cuantificar de algún modo esa posibilidad fundamentada o probabilidad subjetiva.

A la cuestión de si es posible cuantificar matemáticamente la probabilidad estocástica de que suceda un riesgo de seguridad o medio ambiente, nuestra opinión, tras lo estudiado hasta ahora, es que no es posible, o al menos es muy difícil. Nos permitimos llegar a esta conclusión considerando que sobre un posible riesgo de este tipo no disponemos de un espacio muestral definido que permita establecer en su seno la proporción entre casos posibles y favorables. Vamos a verlo intentando su aplicación para calcular la probabilidad de robo en un ámbito determinado.

Hay que definir el ámbito geográfico y temporal sobre el que vamos a estudiar las previsiones.[23] Pero dependiendo del tamaño y características del espacio muestral definido, obtendremos unos u otros resultados sobre la probabilidad de robo y podrán o no servir para extrapolarlos a evaluación del riesgo. No será lo mismo considerar la probabilidad de que roben en una ciudad que en otra, en una ciudad que en una región, en un determinado tipo de empresas que en otro, en una zona conflictiva que en una residencial. Se trata de muestras de características muy diferentes entre sí, lo que hace difícil extrapolar sus resultados. Si se dispusiese de estadísticas fiables, contaríamos con una referencia de la frecuencia de robos en el espacio geográfico, social y temporal que se haya considerado. Pero estaríamos ya más ante un indicio a integrar, que ante un dato probabilístico aplicable para calcular el riesgo de robo en cualquier circunstancia y lugar.

Podemos preguntarnos si sería factible aplicar métodos de técnica actuarial para llegar a la valoración matemática de la probabilidad, planteándonos si sería posible utilizar alguna de las

[23] La regla de Laplace "casos favorables sobre casos posibles" parte de un universo de sucesos basado únicamente en el espacio, la probabilidad de un suceso es la proporción del espacio vinculado al mismo. Ahora planteamos ampliar el universo al espacio-tiempo.

técnicas de prospección, por ejemplo la distribución de Poisson, de Paretto[24], etc. Sobre este particular albergamos también serias dudas, considerando que no se dispone de masa crítica suficiente ya que se trata de sucesos de baja frecuencia, sobre los que apenas existen estadísticas oficiales.[25] Ya hemos expuesto que algunos hemos de considerarlos pese a que no hayan ocurrido nunca (pusimos el ejemplo del sabotaje, podemos mencionar también el riesgo de terrorismo en un lugar que no haya sufrido nunca un atentado, pero que los indicios, informaciones o análisis lleven a la necesidad de controlarlo). Para obtener datos de frecuencia, será necesario ampliar el espacio muestral considerado; pero cuanto mayor sea la amplitud del campo de estudio, menos relevantes serán los datos obtenidos para predecir el riesgo en otros espacios. Dificultad mayor en tanto en cuanto las circunstancias particulares de las muestras no sean coincidentes. Así, con las limitaciones estadísticas expuestas, la frecuencia de robos en toda España, puede ser relevante de cara a predecir su comportamiento futuro, pero referido a España en su conjunto. Resultará complicado aplicar este dato para predecir el robo en una ciudad conflictiva y en otra de bajo nivel de delincuencia. Máxime si lo que necesitamos es un dato para predecir el riesgo en una empresa……

Constatada la dificultad para cuantificar matemáticamente la probabilidad de los riesgos de seguridad y medio ambiente, si pretendemos lograr un método de evaluación cuantitativo, nos vemos obligados a buscar otras soluciones para valorar de forma coherente la probabilidad. En caso contrario, si no lo logramos, habremos de convenir que el riesgo de seguridad no se puede cuantificar, (premisa de la que por cierto, y como ya hemos mencionado parten muchos métodos para evaluar el riesgo operacional).

[24] Desde Solvencia II para el cálculo del riesgo, se propugna la utilización de la técnica actuarial.

[25] EL Ministerio del Interior publica anualmente las estadísticas de delitos en España. Lamentablemente, pueden dar una idea del estado de la seguridad a nivel nacional, pero los datos sobre delitos concretos no permiten llegar a conclusiones sobre la probabilidad de que sucedan. Se trata de datos de delitos probados, dejando fuera los casos no resueltos o absueltos en los tribunales. A lo que cabe añadir lo ya mencionado en el texto sobre la imposible extrapolación de datos obtenidos para un ámbito geográfico a otro más reducido y con circunstancias y vulnerabilidades diferentes.

Podemos optar por una parametrización de la probabilidad basada en criterios cualitativos, a partir de los cuales asignemos valores convenidos. Nótese que ya nos movemos en el campo de la probabilidad subjetiva, no en el de la estocástica o matemática.

Para valorar la probabilidad subjetiva vamos a partir de la integración de evidencias. La consideración a efectos del cálculo del mayor número de éstas, procurando que respondan a criterios objetivos, permitirá reducir la carga subjetiva de nuestro cálculo. Con estos criterios parametrizaremos las evidencias, asignándoles valoraciones. Finalmente se deberá encontrar una regla matemática para integrar las evidencias valoradas en la probabilidad. En paralelo estableceremos también criterios para clasificar la probabilidad ya valorada.

La cuestión se centrará ahora en definir qué evidencias o factores de riesgo nos interesan y cómo los vamos a valorar. Finalmente deberá establecerse una relación matemática que integre todos esos valores en la probabilidad.

Otra cuestión a tener en cuenta es que esta valoración operará o tendrá efectos en el ámbito empresarial o de riesgos para el que se haya definido y en el que se haya admitido como patrón. Fuera de estos ámbitos será creíble en la medida en que el método esté suficientemente explicado y razonado. Y para poder comparar resultados de ámbitos distintos es necesario, que se adopten patrones o reglas de medir, comunes. Cuestión que como vemos es recurrente.

Hemos mencionado repetidamente la necesidad de integrar evidencias, poniendo de relieve que no tiene la misma probabilidad de riesgo un activo que cuente con medidas de seguridad que otro que no disponga de estas, o el que está en una zona conflictiva respecto a que se encuentra en una zona residencial…Estas consideraciones llevan a plantearnos si no estaremos entrando en el ámbito de la probabilidad condicionada, deviniendo aplicables los teoremas de Bayes. Con esta posible solución, el enfoque da un giro para analizar si es factible aplicar las teorías bayesianas y si permitirían para integrar las evidencias, obteniendo un valor para la probabilidad.

4.2.2. Aplicación del Teorema de Bayes al cálculo de la probabilidad de manifestación de los riesgos de seguridad y medio ambiente.

Retomamos el supuesto de un riesgo que nunca se ha producido, pero que si sucediese provocaría un daño de consecuencias muy graves, podemos pensar en muchos riesgos de seguridad que responden a estos parámetros, ya hemos mencionado el sabotaje o el riesgo de terrorismo, cuando no se han producido nunca ni en la empresa ni en el ámbito geográfico donde se ubica. ¿Estaríamos en disposición de manifestar que como nunca se han producido, en éste ni en otros edificios de la compañía, no existen estos riesgos…? Evidentemente la respuesta es no, es necesario considerarlos y gestionarlos. Más aún, algunos, por su propia naturaleza son siempre considerados como graves.[26]

Si a este tipo de riesgos aplicamos el cálculo probabilístico, podemos considerar como casos posibles el conjunto de los edificios de la compañía o los del sector o los que sean pero ¿cuáles son los casos favorables? Dada la baja frecuencia, para encontrar casos favorables ampliaremos el espacio muestral, con lo que los casos posibles aumentarán también proporcionalmente y por tanto en mayor número. El resultado será que la probabilidad matemática de este tipo de riesgos es ínfima. Aplicando una función que relacione ésta con el valor del daño, se obtendrá un valor de riesgo tan pequeño que, si no consideramos otros factores, deberíamos interpretar que se trata de riesgos casi inexistentes para los que no es necesario tratamiento. Lo que contradice la realidad, ya vemos que nuestra percepción es que no podemos dejar de controlar el riesgo de terrorismo, aunque no se haya producido nunca en ese ámbito o el de incendio….

La cuestión a resolver será pues, cómo integrar las evidencias en la valoración de la probabilidad, de modo que aproximemos ésta a la realidad de estos riesgos.

[26] El riesgo de terrorismo, de baja o muy baja incidencia, es generalmente considerado como grave o muy grave. Algunas de las grandes empresas españolas, multinacionales, lo consideran riesgo estratégico al nivel más alto de riesgos de la empresa, aun en el caso de no haber sufrido atentados o en muy baja frecuencia.

A veces, la probabilidad de que un determinado suceso tenga lugar depende de que otro suceso se haya producido o no con anterioridad. Esto es, en ocasiones el hecho de que se produzca un determinado fenómeno puede hacer más o menos probable la aparición de otro. Llegamos así a las **probabilidades condicionadas**, *denotándose por P (A/B) a la probabilidad condicionada del suceso A, suponiendo que el suceso B haya ocurrido ya*.

La resolución de estos casos se consigue aplicando el teorema de Bayes, cuya expresión matemática es la que sigue[27]:

$$P(A/B) = \frac{P(A) \times P(B/A)}{P(B)}$$

Siendo: P(A/B) la probabilidad de que suceda A, condicionada a que suceda B.

P (A) y P (B) las probabilidades a priori de que suceda A o B.

P (B/A): la probabilidad de B si ha sucedido A.

Este teorema exige el conocimiento de una probabilidad *a priori* es decir conocida de antemano (estudios previos, experiencia, opinión de expertos, un ensayo previo o actual) y de los datos obtenidos, seguidamente se procede al cálculo de la *verosimilitud*, y obteniendo finalmente una probabilidad *a posteriori*[28].

Trataremos pues de analizar si aplicando Bayes, podemos valorar, por ejemplo, cuánto más probable es un riesgo que cuenta con medidas que otro en idénticas circunstancias para el que no se han establecido medidas. O donde decimos medidas póngase cualquier otra evidencia que altere o condicione la probabilidad de que ocurra el riesgo, así la conflictividad de la zona, el valor de los activos, etc.

Continuando con el supuesto del probable robo, para aplicar la inferencia bayesiana como método para calcular su probabilidad condicionada a la existencia de medidas de seguridad, es

[27] La Teoría Bayesiana se basa en la enumeración de diferentes eventos posibles y la asociación de cada uno con una probabilidad de ocurrencia. Por medio de la cuantificación del impacto de cada evento, y la multiplicación por su correspondiente probabilidad de ocurrencia, se pueden calcular los "daños esperados" de cada factor de riesgo.

[28] Cabe citar que la Metodología Bayesiana ha encontrado múltiples campos de aplicación: Artillería, juegos de azar, toma de decisiones, evaluación de riesgos, redes neuronales, guías de expertos, etc.

preciso saber, *"a priori"* la probabilidad de que una instalación cuente con medidas; también hay que disponer del dato de la probabilidad de robo si no se cuenta con medidas.
Cuestiones que nos llevan de nuevo a la dificultad para establecer valoraciones matemáticas de probabilidad.

Además, encontramos otros dos tipos de dificultades para aplicar directamente el teorema de Bayes al cálculo de la probabilidad de los riesgos de seguridad y medio ambiente:

- Por una parte tenemos que el número de evidencias que condicionan la probabilidad de los riesgos es muy amplio[29]. Como más significativas podemos identificar entre éstas:

    - La existencia o no de medidas de seguridad.
    - La conflictividad y nivel social de la zona.
    - La representatividad de la instalación.
    - El valor y atractivo de los activos.

- Y por otra parte, nos encontramos de nuevo con el problema de la falta de disponibilidad de estadísticas de riesgos de seguridad. Problema incluso agravado considerando que para aplicar este teorema, no basta conocer los datos referentes al robo, por ejemplo, sino que debe discriminarse entre los robos producidos en locales que cuenten con medidas y en los que no cuenten con estas.

Nos topamos nuevamente con unos problemas de difícil solución para llegar a algún modelo para cuantificar la probabilidad.

Analizando el estado de la cuestión hasta este punto, conocemos evidencias que influyen en la aparición y en la manifestación del riesgo; partiendo de éstas, razonablemente podemos concluir que incrementarán o reducirán la probabilidad de que suceda. Pero no tenemos, o no

[29] Se trataría de una red causal o una red bayesiana

hemos sido capaces de encontrar, una herramienta o método que permita llegar al cálculo matemático de la probabilidad, que se torna necesario para aplicar cualquier método estadístico.

Regresamos pues a la necesidad de parametrizar las evidencias e integrarlas. Recurriremos para ello a establecer patrones y clasificaciones en función de hechos objetivos.

Más, tampoco hemos encontrado el método que nos permita integrar las evidencias. Lo visto hasta ahora no ha resuelto, desde nuestro punto de vista, el problema.

Esta situación, nos ha llevado a proponer los dos métodos de evaluación que se desarrollan en los capítulos siguientes, pretendiendo con ambos desde ópticas muy diferentes, lograr una valoración cuantitativa de los riesgos de seguridad y medio ambiente.

4.3. Sobre la cuantificación del daño.

No puede perderse de vista que el riesgo es función de la probabilidad y del daño. En este capítulo se ha dado cumplida cuenta sobre la situación y perspectivas para valorar la probabilidad. De igual modo hay que analizar si el daño puede o no cuantificarse, y qué dificultades podemos encontrar en esta tarea.

Hemos denominado "daño" a la segunda componente del riesgo, entendemos que este término define más exactamente lo que provoca el riesgo si se manifiesta. Como término equivalente a daño la Guía ISO CEI 73 utiliza "consecuencia"[30] . También se han encontrado métodos y estudios que utilizan la intensidad e incluso la importancia que tiene para la organización.

[30] La consecuencia no siempre tiene por qué ser dañina, se entra así en el concepto del riesgo positivo. Pero el riesgo de seguridad siempre es negativo. Así lo define la Guía ISO CEI 73. Por este motivo para evaluar el riesgo de seguridad se prefiere el término "daño" en lugar de "consecuencia". Si bien más allá de la cuestión terminológica, esta diferencia no altera el carácter ni el fondo del asunto.

Nuestra opinión al respecto es que el término daño englobaría al resto, con el matiz del riesgo positivo para cuya consideración se ha de utilizar "consecuencia" (ver nota 29).

El daño es cuantificable por lo general, con excepciones como el producido a los activos intangibles, de muy difícil valoración.

La cuantificación del daño o las consecuencias del riesgo, deben analizarse partiendo de la identificación de escenarios posibles. Se llegará al análisis de cada situación y en qué medida afecta.

Al contrario de lo que ocurre con la probabilidad, para cuantificar el daño sí se dispone de métodos efectivos con un buen nivel de objetividad. Al desarrollo de estos métodos se ha contribuido de manera decisiva desde el ámbito asegurador. Gozando de gran predicamento en cuanto a la técnica aseguradora los utilizados para el valorar las posibles pérdidas ocasionadas por un siniestro.

Entre estos métodos cabe mencionar los utilizados para calcular sistematizadamente las pérdidas: la Pérdida Máxima Posible (PML, Possible Maximum Loss), la Pérdida Máxima Probable (MPL, Probable Maximum Loss), Pérdida Máxima Absoluta (AML, Absolute Maximum Loss), etc.

Esta favorable situación con la que nos encontramos, no puede dejarnos la idea de que valorar el daño o la consecuencia es tarea fácil.

Hemos mencionado el daño a los intangibles, como a la imagen, a la marca, el daño reputacional, etc. Por la propia naturaleza de los activos, de difícil valoración, será también muy difícil llegar a valorar el daño.

4.3.1. Identificación de escenarios

Para valorar los daños posibles es necesario identificar los escenarios posibles, habrá que "visualizar" el contexto en que se manifestaría el riesgo y los activos a los que afectaría.

Se dispone también de metodología, admitida y aplicada regularmente en el campo asegurador, para calcular el daño en cada escenario. Se parte de aplicar parámetros como proximidad, naturaleza del bien, fuente y naturaleza del riesgo, etc.

Dado que se cuenta con estos métodos que ofrecen un funcionamiento aceptable, no se ha estimado necesario profundizar desde este trabajo en cuanto a métodos de valoración del daño.

4.3.2. Valoración de activos

La valoración de activos va indisolublemente unida a la valoración de daños. Obviamente, el daño no tiene entidad propia si no es referido a un activo. Consecuentemente, no puede entenderse ninguna referencia a los riesgos sin tener en cuenta los activos a los que afecta.

Genéricamente los activos sobre los que actuará la seguridad (lógicamente disponiendo lo necesario para protegerlos controlando los riesgos que les afecten o les puedan afectar) pueden clasificarse en estos grupos:

- Personas.
- Información.
- Imagen.
- Activos patrimoniales tangibles.
- El propio negocio como objeto a garantizar.

Identificar y valorar todos los activos, es como significábamos tarea difícil. Los métodos mencionados para valorar las pérdidas, están basados en el valor de los activos. Su aplicación deberá ser más o menos exhaustiva dependiendo de la aptitud y apetencia del riesgo.

Estimamos en cualquier caso necesario que junto a la identificación de riesgos se lleve a cabo una identificación de activos, marcando de forma especial aquellos valiosos que no formen parte del patrimonio esperado. Nos referimos a casos como detectar obras de arte valiosas en un edificio, o equipos electrónicos de gran valor, etc., que habrán de marcarse con especial atención.

Cabe significar que la valoración exhaustiva y detallada de los activos, será necesaria para desarrollar otras fases de gerencia y para tomar la decisión sobre el tratamiento del riesgo.

4.3.3. Aspecto subjetivo del daño

Con este enfoque pretendemos poner de relieve, el hecho cierto de la diferente percepción del daño dependiendo de la organización que lo sufra.

Como viene siendo habitual en este trabajo, recurrimos una vez más a un ejemplo sencillo y significativo. Supongamos que se ha producido el robo de un ordenador en una empresa de servicios, quizá el único trastorno que le cause sea la pérdida patrimonial derivada de su coste; considerando la facilidad de reposición, el resto de inconvenientes se solventan adquiriendo otro. Pero si el robo de un ordenador similar se produce en una empresa de investigación y desarrollo, puede ser considerado como grave en función, por ejemplo, de la información que pueda contener. Es cierto que estaríamos ante hechos diferentes (robo de equipo frente a robo de información sensible), pero precisamente esto llevará a que la misma acción sea considerada de forma diferente en cada organización.

Más evidente puede ser la aptitud ante una pérdida puramente patrimonial. Si un riesgo determinado provoca una pérdida de 300.000 euros, para una gran empresa con facturaciones

de muchos millones de euros no supondrá el mismo inconveniente, ni tendrá las mismas consecuencias, que para una pequeña empresa familiar, que puede verse abocada incluso a la desaparición.

Esto lleva a la necesidad de contar con un pronunciamiento previo de la empresa u organización sobre su apetencia al riesgo. Recordemos lo expuesto cuando tratamos el tema de la Política de Riesgos, muy necesaria en la empresa.

En paralelo, unido a este aspecto subjetivo del daño, no puede pasar desapercibido, el hecho de que, el daño o las consecuencias, a su vez pueden configurarse como integración de varios factores, pudiendo mencionar entre estos:

- Los ya aludidos de la cuantía de las pérdidas.
- Las consecuencias que va tener para la empresa, diferentes de las que pueda provocar en otra.
- Las pérdidas intangibles.
- ….

De forma equivalente a lo que concluimos para integrar las evidencias de probabilidad, tendremos que llegar a una integración de los factores que condicionan el daño. Y como en aquella ocasión, no se dispone de un método que integre de forma sistemática esos posibles factores.

Pero repetimos, estas carencias se suplen en gran parte con los métodos desarrollados en el sector asegurador, para cuantificar las posibles pérdidas ante un siniestro.

CAPÍTULO 5. APUNTES PARA EL ANÁLISIS VECTORIAL DEL RIESGO. PROPUESTA DEL MÉTODO VECTORIAL PARA LA EVALUACIÓN DE RIESGOS COMO INTEGRADOR DE EVIDENCIAS Y FACTORES DE RIESGO[31].

5.1. Justificación de una nueva metodología.

Tras lo analizado hasta el momento, los métodos vistos no satisfacen nuestras necesidades para alcanzar una valoración de los riesgos de seguridad y medio ambiente lo más científica posible y de carácter universal, esto es, que sea aplicable a un espectro importante de riesgos y en un gran número de situaciones. Hemos buscado métodos que permitiesen cuantificar el riesgo, partiendo de la valoración de factores como la probabilidad y la intensidad, consecuencias o daño; no los hemos encontrado.

Ya apuntamos que como opción, quedaba elaborar un sistema de parametrización para los factores de riesgo, suficientemente explícito y definido, de forma que la carga subjetiva quedase reducida en lo posible.

Por otra parte, analizando el concepto del riesgo y su concepción matemática. Hemos albergado serias dudas sobre su concepción como esperanza matemática, al menos en lo referente al riesgo de seguridad. Pero también se ha comprobado cómo los diversos métodos formulan la función matemática que conviene a sus necesidades. De forma análoga, una formulación diferente a las utilizadas hasta ahora, estaría justificada en la medida en que sea coherente y razonada y constituya un instrumento óptimo para la evaluación.

[31] Sin entrar en otras disquisiciones hacemos equivaler los términos "evidencia" y "factor de riesgo", pretendiendo englobar con ambos todo lo que influye o afecta al riesgo incrementándolo, referido sobre todo a la probabilidad.

Percibimos la necesidad de integrar las evidencias o los factores de riesgo, como vía para incorporar a la evaluación todo aquello que percibimos como decisivo de cara al riesgo, pero que desde la concepción probabilística quedaba fuera. Constatamos también que métodos como los Bayesianos, a salvo de estudios más profundos sobre el tema, en las circunstancias en que nos movemos y dentro del ámbito del riesgo de seguridad, no son fácilmente aplicables. Echando mano de los métodos tradicionales para evaluar el riesgo de seguridad, se ha puesto de manifiesto su imposible aplicación en muchos casos y sus limitaciones para integrar factores diferentes de los que propone.

Lo anterior ha motivado que entre los objetivos de este trabajo se haya incluido el de obtener una relación matemática, que respetando la concepción del riesgo, recoja e integre las evidencias y permita llegar a una valoración de los riesgos de seguridad y medio ambiente. Así se ha iniciado el camino del riesgo concibiéndolo como vector, aplicando las reglas del espacio vectorial a su cálculo. Camino, incierto desde el punto de vista científico por inexplorado aún, y en el que este trabajo sólo pretende ser el punto de partida.

Por otra parte, fruto de esta ausencia de metodología apropiada, las representaciones gráficas mediante mapas de riesgos presentan, a nuestro juicio, importantes deficiencias; aun recurriendo a la formulación primigenia del riesgo como factor de la probabilidad por la intensidad. Entre estas destacamos la dificultad para recoger gráficamente el valor del riesgo, ya que no relacionan su posición relativa con su valor.

Con el fin de superar esta situación, en este trabajo se propone el nuevo método vectorial de evaluación que se expondrá.

Se parte de la necesidad de lograr un método que permita:

- Su aplicación a la práctica totalidad de riesgos de seguridad y a los de medio ambiente como primera valoración base para sus métodos específicos.

- Integrar las evidencias. Posibilitando la utilización de un amplio catálogo de criterios. No puede tratarse de un método a partir de criterios encasillados e inamovibles.
- Reducir a lo mínimo posible la carga subjetiva del evaluador. Se aproximará por tanto a los métodos cuantitativos en la medida de lo posible.
- Que los valores de riesgo que se obtengan sirvan para comparar, verdaderamente, los riesgos entre sí, con la posibilidad de establecer prioridades de actuación en función únicamente de la valoración obtenida.
- El nuevo método deberá posibilitar la representación del riesgo en un eje de coordenadas, en función exclusivamente de su valor absoluto, posibilitando la integración de múltiples factores en ese valor y su representación gráfica.
- Además de lo referente a la valoración este nuevo método deberá dar respuesta a todas las fases de la evaluación de riesgos, incluyendo el tratamiento.

Con estas premisas se propone el método que se describe.

5.2. Concepción vectorial del riesgo. Integración de evidencias.

5.2.1. Formulación Matemática del Vector Riesgo

Como se ha indicado, se parte de la concepción del riesgo como combinación de la probabilidad de un suceso y de su consecuencia, definición recogida por la Guía ISO / CEI 73, y comúnmente admitida.

Nos vamos a apartar de la concepción del riesgo, muy generaliza, como expresión de una esperanza matemática, lo que lleva a su función como el producto de la probabilidad y la

intensidad, (o el daño o la consecuencia.)[32]. En el capítulo precedente se ha analizado si los riesgos de seguridad y medio ambiente pueden participar de esa concepción como esperanza matemática, exponiendo nuestras dudas, al menos razonables, al respecto. Considerando además, que, como también se recoge en el capítulo anterior, ninguno de los métodos analizados aplica para el cálculo dicha función en puridad, por lo que este hecho no puede constituir motivo de rechazo del aquí propuesto.[33].

La necesidad de encontrar una función que relacione el valor del riesgo con su posición relativa respecto a un eje de coordenadas, nos llevó a indagar sobre su posible concepción como vector.

En suma lo que se está buscando es una función matemática que defina el riesgo en relación con su distancia el origen de coordenadas. Esta función, por otra parte, debe considerar los parámetros de probabilidad y daño.

La función que responde a lo anterior es la que calcula la modulación del segmento que une el origen con el punto (p, d), de coordenadas la probabilidad y el daño.

Esta función, aplicando el teorema de Pitágoras, y normas del espacio vectorial, es la raíz cuadrada de la suma de los cuadrados de la probabilidad y el daño[34].

$$R\,f\,(P,D) = \sqrt{(P^2 + D^2)}$$

[32] Como se ha indicado anteriormente, para este estudio se utilizará indistintamente el concepto de consecuencia de daño o de intensidad, cuestión que no va a incidir en el concepto del riesgo.

[33] Para la mayoría de los autores el concepto de riesgo se define a partir de la relación entre probabilidad y consecuencia, sin definir la función. Como ejemplo de lo manifestado, en la obra "Manual de Evaluación y Administración de Riesgos", de la editorial Mc Graw Hill, de varios autores ya citados, referente a los riesgos ambientales expresa: "En concepto el riesgo se refiere a la probabilidad condicional de la ocurrencia de un acontecimiento especificado, combinado con alguna evaluación de las consecuencias del acontecimiento" (Pág. 10-4 .Óp. citada).

[34] La formulación del riesgo como raíz cuadrada de sumatorios de cuadrados, si bien no directamente, sí ha sido utilizada por algunos métodos; así se ha encontrado para n diagnósticos de seguridad tecnológica, definiendo el riesgo global como raíz cuadrada del sumatorio del cuadrado de los valores obtenidos para los riesgos referentes a cada una de las tres áreas sobre las que actúa. (ORACLE)

La representación gráfica del riesgo en el eje de coordenadas sería:

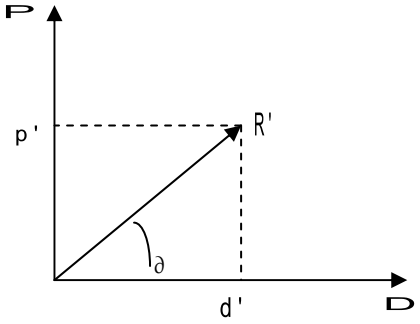


Fig. 7. Vector Riesgo.
Fuente: Elaboración Propia

Definimos así el riesgo como el vector con origen el origen de coordenadas (0,0) y extremo el punto (p, d), siendo d el valor del daño y p el valor de la probabilidad.

El módulo del vector riesgo $R^{\rightarrow}$ será la raíz cuadrada de la suma de los cuadrados de la probabilidad y el daño.

$$\left| R^{\rightarrow} \right| = \sqrt{(P^2 + D^2)}.$$

La dirección del vector $R^{\rightarrow}$ vendrá dada por el ángulo ∂, cuyo valor es:

$$\partial = \text{arc.tg } P / D$$

Así, todo riesgo quedará especificado por su valor absoluto, expresado por el módulo del vector, y dependerá de la distancia al origen de coordenadas y por su dirección que vendrá dada por la proporción entre los valores de la probabilidad y el daño.

Dos riesgos del mismo valor, podrán tener dirección diferente. Veremos que esta característica adquiere importancia de cara a la prioridad del tratamiento. De esta forma, el riesgo quedará definido por su valor y por la relación entre probabilidad y daño, sin necesidad

de acudir a otras caracterizaciones como grosor del punto, color, etc., para clasificarlos y representarlos.

A partir de esta definición vectorial del riesgo, se diseñará un método de evaluación que responda a las premisas marcadas; entre éstas la necesidad de que los valores obtenidos sean directamente comparables entre sí,[35] permitiendo su representación en un eje bidimensional de coordenadas.

5.2.2. Interpretación gerencial de la dirección del Vector Riesgo

Se ha definido el Vector Riesgo, $\vec{R}$, se ha calculado su módulo y se ha identificado su dirección como el ángulo ∂, expresado como el arcotangente del valor de la probabilidad partido por el valor del daño o la intensidad.

Considerando que todo vector tiene que definirse por su módulo y su dirección, se consigue así la definición del Vector Riesgo, $\vec{R}$.

Resulta interesante interpretar el significado de la dirección de este vector $\vec{R}$ desde el enfoque de la gerencia, dilucidando las posibles implicaciones en el tratamiento del riesgo.

El módulo del vector o valor absoluto del riesgo, va a permitir una primera clasificación de los riesgos en tramos, de acuerdo con su cuantía. El gerente de riesgos dispone así de una herramienta que le permitirá decidir si acomete el tratamiento de unos u otros riesgos en función de su valor.

El problema podría plantearse cuando se encuentre frente a riesgos de igual cuantía pero con diferente relación entre la probabilidad y la intensidad o daño.

Si consideramos un riesgo R1, de probabilidad 3 e intensidad 4, aplicando este método, su valor será: $R1 = \sqrt{(3^2 + 4^2)} = 5$.

[35] Sin perjuicio de que también se puedan comparar por el resto de los factores que integren el riesgo evaluado.

Si consideramos otro R2 de probabilidad 4 e intensidad 3, su valor será igualmente 5.

Podría preguntarse cuál de los dos es más prioritario para acometer su tratamiento. La decisión dependerá de la aptitud de la organización ante el riesgo, debiendo decidir si a igualdad de riesgo se afrontan antes los más probables o los más dañinos.

La dirección del vector va a indicar la relación que existe entre la probabilidad y el daño; así cuanto mayor sea el ángulo ∂, mayor importancia relativa tendrá la probabilidad en la configuración del riesgo. Por el contrario en la medida en que el ángulo ∂ sea menor, estaremos ante riesgos más dañinos pero menos probables.

Este indicador puede incluirse como un factor más para clasificar los riesgos, aportando en el Mapa de Riesgos una visión rápida de cara a priorizar el tratamiento del riesgo.

En la representación se puede apreciar cómo dos vectores R y R', de igual valor, pero con direcciones diferentes dadas por los ángulos α y β, tienen diferentes relaciones de probabilidad y daño.

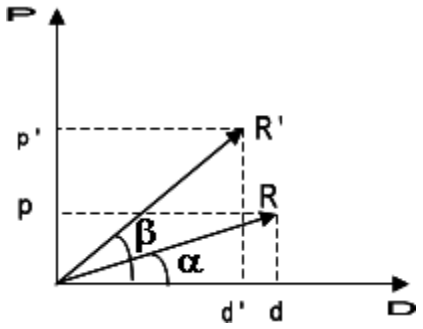


Fig. 8. Dirección del vector en relación con la probabilidad y el daño.
Fuente: Elaboración Propia.

5.2.3. Definición del riesgo en función de las evidencias o factores de riesgo. La integración de evidencias.

Si se conociese el valor de la probabilidad y el del daño o la consecuencia, directamente por aplicación de la fórmula anterior, obtendríamos el valor del riesgo[36].

Pero estamos buscando una metodología que reduzca al máximo posible la subjetividad. Desde este punto de vista, se reducirá el factor subjetivo en tanto en cuanto se introduzcan en el cálculo del riesgo más factores, parametrizados en función de criterios claros y precisos; descartando indefiniciones y cuestiones que no respondan a la realidad.

Si únicamente se calculase la probabilidad en función de cualquier gradación que se pueda proponer, sin definir qué otros factores influyen en la misma, se estaría introduciendo un criterio subjetivo que invalidaría el método de evaluación. Idéntico razonamiento se sigue para el daño o consecuencia.

Por este motivo, el valor tanto de la probabilidad como del daño o consecuencia, se va a hacer depender a su vez de otros factores en la medida en que sea posible párametrizarlos.

Conviene también traer a colación todo lo tratado en el Capítulo 4, en cuanto a la necesaria integración de las evidencias de riesgo[37] . Quedó claro que la percepción que se puede tener del riesgo, motivada por esas evidencias, no siempre va a coincidir con un posible cálculo probabilístico[38]. Uno de los objetivos de esta metodología es precisamente, la integración de evidencias.

[36] Como se ha puesto de manifiesto repetidas veces, obtener el valor matemático de la probabilidad para riesgos de seguridad es tarea muy difícil, sino imposible.
[37] Sin entrar en otras disquisiciones hacemos equivaler los términos "evidencia" y "factor de riesgo", pretendiendo englobar con ambos todo lo que influye o afecta al riesgo incrementándolo, referido sobre todo a la probabilidad.
[38] Ib nota anterior.

La probabilidad como parámetro [39]

Esta propuesta aplica dos factores nuevos como conformadores de la probabilidad, considerando que la probabilidad de que se manifieste un riesgo determinado, será función de[40]:

- La frecuencia con la que ya se haya manifestado el riesgo. (Fr).
- Las vulnerabilidades que lo hagan más posible. (V) teniendo en cuenta para valorar la vulnerabilidad la existencia o no otros factores que pueden incrementar o disminuir la posible manifestación del riesgo, como existencia o no de medias de seguridad óptimas, la conflictividad de la zona, etc.

La expresión matemática de la probabilidad será a su vez función exponencial de la frecuencia y de la vulnerabilidad.

La "vectorización" de esta función, aplicándole al menos el concepto de módulo para calcular su valor, permite su cuantificación exacta a partir de los valores predeterminados de frecuencia y vulnerabilidad. Cuantificación que, por otra parte, permite comparar las diferentes probabilidades, estableciendo su gradación en función de la resultante de los dos parámetros mencionados.

La expresión matemática de la probabilidad de manifestación de un riesgo identificado, en función de la frecuencia y de la vulnerabilidad, se expresa mediante la siguiente fórmula:

$$\mathbf{P\ f\ (Fr,\ V) = \sqrt{(Fr^2 + V^2)}.}$$

[39] No se aplica el concepto estadístico de la probabilidad, ya que en muchas ocasiones será imposible conocer el número de casos favorables y el total de posibles. Ver capítulo 4 y notas precedentes.

[40] En esta propuesta se han considerado estros dos aspectos como decisivos de cara a la probabilidad, pero, como ya se verá, no se trata de un método cerrado, posibilitando que a juicio del evaluador, se introduzcan otros factores, con la condición de que se hayan parametrizado previamente.

Definiéndose así la ***probabilidad*** *como la raíz cuadrada de la suma de los cuadrados de la frecuencia y la vulnerabilidad*.

A continuación se dan las pautas para parametrizar la frecuencia y la vulnerabilidad.

Valoración de la frecuencia.

La frecuencia es el número de veces que se repite un suceso[41].

En el ámbito de la gerencia de riesgos, para valorarlos, es importante conocer las veces que se ha manifestado el riesgo. Se entiende un parámetro fundamental, ya que traslada el riesgo desde el plano teórico al real, considerando lo que ya ha sucedido, permitiendo un análisis más objetivo y ajustado a la realidad.

Resulta evidente que no es lo mismo valorar el riesgo de intrusión en un edificio, en el que nunca han entrado, que valorarlo si se conoce que ya se ha producido la intrusión en alguna ocasión o que se ha producido varias veces. Debidamente parametrizada, la frecuencia de aparición puede proyectarse como previsión de la manifestación del riesgo.

Así la probabilidad de que un riesgo se manifieste va a ser función también de la frecuencia con que haya sucedido[42].

Concepto y parametrización de la vulnerabilidad[43].

Por vulnerabilidad se entiende la debilidad, disposición interna o circunstancia de la instalación o del bien, que incrementa la posibilidad de que se manifieste un determinado riesgo.

[41] Definición de la Real Academia de la Lengua.
[42] Erróneamente, muchos métodos de evaluación identifican directamente probabilidad con frecuencia.
[43] El concepto de vulnerabilidad es el utilizado en las Instrucciones Técnicas de Seguridad Integral de la Fundación MAPFRE. "Terminología Básica de Seguridad Integral" Abril 2004.

En el concepto de vulnerabilidad adoptado aquí, se engloban todos aquellos factores que operan como atrayentes del riesgo, así la existencia o no de medidas de seguridad, su eficacia, la conflictividad de la zona, etc.

La vulnerabilidad como parámetro puede a su vez, hacerse depender matemáticamente de un número ilimitado de factores que, evidentemente, influyen en la misma.

Por el mismo motivo expuesto sobre la valoración de la frecuencia, se propone un modelo para valorar la vulnerabilidad, bien entendido que el evaluador podrá adoptar otras valoraciones que se ajusten más a su realidad.

Factores o evidencias de daño[44]

Por daño se considera el impacto que tiene en la compañía u organización la manifestación del riesgo.

Este concepto plantea la relatividad del daño, dependiendo de lo que le suponga a la empresa u organización concreta. Así el daño que ocasiona a una gran empresa una pérdida de 100.000 euros va a ser menor que el que le ocasiona a una empresa familiar. Por este motivo, cada empresa deberá adoptar su propia clasificación del daño. La pretensión es proponer unos criterios para valorarlo y a partir de estos, por ser necesario para la exposición de esta metodología de evaluación, se parametriza y clasifica.

Para valorar el daño se tendrán en cuenta factores como la influencia en el negocio, las pérdidas económicas, el valor de los daños materiales, posibles daños a las personas, la facilidad de reposición, y las repercusiones en intangibles como la pérdida de imagen.

[44] Ver en Capítulo 4, el punto 4.4. Sobre cuantificación del daño.

Integración de los factores o evidencias en la expresión final del riesgo. Expresión matemática final del riesgo

El valor del riesgo como función de la probabilidad y del daño, quedó establecido matemáticamente, a partir de la concepción vectorial del riesgo, como:

$$\mathbf{R\ f\ (P, D) = \sqrt{(P^2 + D^2)}.}$$

Como función para determinar la Probabilidad en función de la frecuencia y de la vulnerabilidad (2) se consideró: $\mathbf{P= \sqrt{(F^2 + V^2)}}$ **(2)**

Sustituyendo en (1) por (2), obtenemos la expresión del riesgo en función de la frecuencia y la vulnerabilidad

$$\mathbf{R= \sqrt{(P^2 + D^2)} = \sqrt{((F^2 + V^2) + D^2)}}\ \textbf{, considerando que}\ \mathbf{P= \sqrt{(F^2 + V^2)}}$$

Si el daño a su vez se hace depender de otros factores como su coste (C) y el impacto (I), de tal forma que:

$$D= \sqrt{(C^2 + I^2)},$$

El Riesgo quedaría:

$$R= \sqrt{(F^2 + V^2 + C^2 + I^2)}$$

Y las sucesivas descomposiciones de cada factor en otros, por ejemplo si la vulnerabilidad la hacemos depender de la valoración numérica o parametrización de las medidas existentes, llamémosle M y de la valoración de la conflictividad social de la zona, Z.

Así la vulnerabilidad como función de las medidas de protección y de la conflictivita de la zona sería: $V= \sqrt{(M^2 + Z^2)}$

Si se aplica esta nueva ecuación de la vulnerabilidad a la expresión matemática del riesgo, se obtiene la siguiente expresión del valor del riesgo sería:

$$R= \sqrt{(F^2 + M^2 + Z^2 + C^2 + I^2)}$$

Dónde:

F: Frecuencia de aparición.

M: Valoración de las medidas de protección.

Z: Valor de la conflictividad de la zona y el entorno.

C: Coste monetario del daño.

I: Valor del impacto del daño.

Y a su vez, como otro paso nuevo, podrá descomponerse cada uno de estos factores en otros dos que constituirán sus componentes cartesianas o proyecciones, como raíz cuadrada de la suma del cuadrado de los dos factores.

Tras sucesivas descomposiciones, haciéndolo extensivo, se llega a enunciar como ecuación matemática del riesgo en función de múltiples factores, la siguiente función, como

expresión matemática final del riesgo:

$$R = \sqrt{\left(\sum^{1,n} fi^{2} \right)}$$

Siendo f los parámetros cuantificados que se consideren, y n el número de parámetros.

Así **el riesgo en función de sus evidencias o factores se define:**

"El valor del riesgo será la raíz cuadrada de la suma de los cuadrados de los factores de riesgo, parametrizados, que se consideren".

5.3. Propuesta del método vectorial para evaluación de riesgos

5.3.1. Fases del método propuesto

El método propuesto para evaluar riesgos de seguridad y medio ambiente, consta de las siguientes fases generales:

1. Identificación y Análisis.
2. Evaluación.
3. Clasificación del riesgo.
4. Propuesta de tratamiento.
5. Representación gráfica o mapa de riesgos.

Se describen a continuación cada una de estas fases.

5.3.2. Identificación y Análisis de Riesgos

Proceso por el que se encuentran, enumeran y caracterizan elementos de riesgo[45].

En esta fase, se identificarán todos los riesgos posibles, independientemente del daño que puedan causar o de su probabilidad de ocurrencia. Dentro del ámbito de seguridad y medio ambiente.

Procedimiento propuesto:

- **Recopilación de documentación:**
  - Sobre incidentes: antecedentes de la propia instalación, de la empresa, del sector, de la zona.
  - Sobre el grado de delincuencia de la zona.
  - Histórico de siniestralidad.
  - Recopilación de la documentación disponible referente a seguridad y medio ambiente en la instalación: de los sistemas de seguridad, de los procedimientos y protocolos de seguridad. Procedimientos medio ambientales.
  - Planes de autoprotección y emergencia.
  - Informes de auditorías.
  - Planimetría de la instalación.
- **Visita de Inspección. Trabajo de campo**
  - Preparación.
  - Check List de seguridad y medio ambiente.

[45] Definición de identificación de riesgos recogida por la Guía ISO/CEI 73 Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas.

Análisis del Riesgo

Se entiende por análisis de riesgos el uso sistemático de la información obtenida en la fase de identificación para identificar fuentes y para calcular riesgos. El análisis de riesgos proporciona una base para la evaluación, el tratamiento y la aceptación de riesgos[46].

De la mera identificación de riesgos se pasa al análisis, tras la sistematización de la información "en bruto", relacionándola con sus causas o factores de riesgo. El resultado del análisis se plasmará en un informe de análisis que dará paso a la evaluación de riesgos.

En ocasiones y para algunos métodos, el análisis se confunde con la propia evaluación, ciertamente puede llegar a ser una evaluación cualitativa, pero en ningún caso puede sustituir a la evaluación como proceso para valorar el riesgo en términos comparativos.

5.3.3. Evaluación de riesgos

Es necesario aclarar que las valoraciones que se presentan, solamente responden a un criterio práctico. Como veremos el hecho de que unas se integren como factores de las otras, obliga a la interdependencia de la parametrización. Quiere esto decir que partiendo de los diferentes valores establecidos para la probabilidad (valoración cualitativa de la que se han hecho depender valores numéricos), se establecerán los posibles rangos de valoración de los factores que la integran. Todo ello según este método particularizado. La aplicación de esta metodología, por diferentes empresas u organizaciones, entendida como propuesta de procedimiento, no implica la asunción necesaria de la parametrización establecida.[47]

[46] Definición de análisis de riesgos recogida por la Guía ISO /CEI 73.
[47] Ver capítulo 4 en cuanto a la necesidad de un pronunciamiento sobre la aptitud de la empresa frente al riesgo, que llevará a su vez a establecer una clasificación propia de los factores en función de la gravedad estimada.

Definición de Factores que Integran el Riesgo

Si se conoce el valor de la probabilidad y /o del daño, se aplicará directamente la fórmula:

$$R\ f\ (P,D) = \sqrt{(P^2 + D^2)}$$

Que como hemos visto permite obtener directamente el valor del riesgo a partir de la probabilidad y el daño.

Pero también ha quedado sentado que, puesto que no se dispone de métodos para obtener una probabilidad matemática, hemos acudido a varias evidencias previamente parametrizadas.

Por este motivo, el valor de la probabilidad se hace depender de la valoración previa de la frecuencia y de la vulnerabilidad.

Parametrización de la frecuencia.

En el ámbito de la gerencia de riesgos, en cuanto a la valoración de los mismos, consideraremos las veces que se ha manifestado el riesgo. Se entiende muy importante este parámetro para analizar y valorar debidamente el riesgo, ya que traslada el riesgo desde el plano teórico al real, considerando lo que ya ha sucedido.

Proponemos una graduación de la frecuencia, basada en conceptos lo que la hacen aplicable en las organizaciones en general. No obstante, con el fin de presentar un método en todo su amplitud, se establece una parametrización de la frecuencia, bien entendido que el evaluador podrá adoptar sus propias graduaciones.

La frecuencia se clasificará de acuerdo con la siguiente escala que va desde una frecuencia de 0,1 (no ha ocurrido nunca) hasta una frecuencia de 5 (para un hecho muy frecuente en la empresa), de este modo, *Tabla N. 4:*

Valor	Frecuencia	Descripción
0,1 - 1	Muy Baja.	No ha ocurrido nunca, ni se tienen noticias de que haya ocurrido incluso fuera de la organización. Nada frecuente.
1,1 - 1,99	Media.	Ha ocurrido alguna vez, pero no en la propia empresa.
2 – 3,99	Alta.	Ha ocurrido alguna vez en la empresa y /o algunas vez en un entrono próximo o parecido al de la empresa.
4 - 5	Muy Alta.	Ha ocurrido varias veces en la propia empresa. Es muy frecuente.

Concepto y parametrización de la vulnerabilidad[48].

En la vulnerabilidad influyen todos aquellos factores que operan como atrayentes del riesgo, así la existencia o no de medidas de seguridad, su eficacia, la conflictividad de la zona, etc.

La vulnerabilidad como parámetro puede a su vez, hacerse depender matemáticamente de un número ilimitado de factores que, evidentemente, influyen en la misma. Cuantos más factores se consideren más objetivo serán los resultados obtenidos, pero por criterios prácticos y para facilitar su aplicación, se ha optado por valorar cualitativamente la vulnerabilidad por parte del analista, a partir de la consideración de varios aspectos que pueden hacer más o menos vulnerable el bien que se está considerando.

La presente propuesta es una graduación de la vulnerabilidad en una escala de 0,1 a 5, iría desde la práctica ausencia de vulnerabilidad, 0,1 (la ausencia total de vulnerabilidad, 0,

[48] El concepto de vulnerabilidad es el utilizado en las Instrucciones Técnicas de Seguridad Integral de la Fundación MAPFRE. "Terminología Básica de Seguridad Integral" Abril 2004.

equivaldría a una situación de seguridad total que no existe conceptualmente), hasta una vulnerabilidad absoluta (5) carente de cualquier medida de protección que operan incrementando en grado máximo la posibilidad de que se manifieste el riesgo.

Así se considera, la parametrización de la vulnerabilidad que se recoge en la *Tabla N. 5*

Valor	Vulnerabilidad	Descripción
0,1 - 0,99	Inexistente	Disminuye la posibilidad de aparición. Se consideraría en los casos en que cuente con medidas de seguridad muy efectivas en ausencia de otras vulnerabilidades de cualquier tipo y si además, la zona no es nada conflictiva, con ausencia de otros factores que puedan incidir en la materialización del riesgo. **(Vi).**
1 - 1,99	Baja	Se considera que una instalación o activo es vulnerable a un riesgo en grado bajo, si cuenta con medidas mejorables, la conflictividad de la zona es baja y no hay otros factores que incrementen el riesgo. **(Vb).**
2 - 3,99	Media	Las medidas son insuficientes, obsoletas o poco efectivas. La zona es de una conflictividad normal, o se detectan circunstancias atrayentes del riesgo (como conflictividad laboral, valor de los activos, etc.). **(Vm).**
4 - 5	Alta	Ausencia de medidas o claramente insuficientes para el riesgo en esas circunstancias. Zona de gran nivel de delincuencia. Se constata la presencia de otros factores que operan como multiplicadores del riesgo. **(Va).**

Parametrización de la probabilidad.

El enunciado de la probabilidad, en función de la frecuencia y de la vulnerabilidad, una vez acotados numéricamente estos parámetros serían:

$$\mathbf{P\ f\ (Fr,\ V) = \sqrt{(Fr^2 + V^2)}.}$$

$$\mathbf{P\ f\ (Fr\ 0{,}1\text{-}5,\ Vi0{,}1\text{-}5) = \sqrt{(Fr^2 + V^2)}.}$$

Obteniendo la Probabilidad como función de la frecuencia para valores de 0,1 hasta 5 y de la vulnerabilidad para valores de 0,1 a 5. Siendo esta función la raíz cuadrada de la suma de los cuadrados de ambas magnitudes.

Sus valores posibles serán desde 0,1 (muy poco probable) hasta 7 (muy probable, casi cierto).

La gradación de la probabilidad de que ocurra un riesgo determinado, con su interpretación, es como se recoge en la *Tabla N. 6*:

Valor	Probabilidad	Descripción
0,1 – 1,99	Muy Baja	Difícilmente va a ocurrir. Es posible pero no se conoce que haya ocurrido nunca. **(PMB).**
2 – 3	Baja	Puede ocurrir alguna vez. Se conocen casos, ajenos a MAPFRE en los que ha ocurrido alguna vez. **(PB).**
3,1 – 5	Media	Se considera que ocurrirá a medio plazo. Se trata de riesgos que ya se han manifestado en MAPFRE o en la zona de la instalación. **(PM).**
5,1 – 6,5	Alta	Ha ocurrido más de una vez y es muy posible que vuelva a ocurrir. **(PA).**
7	Muy Alta	Ocurrirá casi con total seguridad. **(PMA).**

Parametrización del daño. Criterios de valoración

Recordemos que por daño se considera el impacto que tiene en la compañía u organización la manifestación del riesgo. Ya se ha analizado la carga subjetiva del daño, y la diferente percepción que pueden tener del mismo diferentes empresas. También se vio cómo un mismo daño puede tener consecuencias diferentes en diferentes organizaciones. Con estas limitaciones, se busca proponer unos criterios para valorarlo y a partir de estos, por ser necesario para la exposición de esta metodología de evaluación, se parametriza y clasifica.

Para valorar el daño se tendrán en cuenta factores como la influencia en el negocio, las pérdidas económicas, el valor de los daños materiales, posibles daños a las personas, la facilidad de reposición, y las repercusiones en intangibles como la pérdida de imagen.

La gradación propuesta es mediante la siguiente escala del 1 al 5. *Tabla N. 7*:

Valor	Valor del daño	Descripción
1 - 1,99	Poco dañino	Leve pérdida económica o material, fácilmente reponible. Afecta muy poco al negocio. El valor económico no supera los 10.000 euros.
2 - 2,99	Dañino	Afecta de forma importante a una Unidad u Oficina. Afecta, al menos localmente, a la imagen. El valor económico es entre 10.000 y 100.000 euros. Puede provocar daños a las personas.
3 - 3,99	Bastante dañino	Importantes pérdidas que pone en riesgo la actividad de un área. Paralizan al menos temporalmente una parte del negocio. No es de fácil reposición. Riesgo importante para las personas. Repercute a nivel nacional en la imagen. El valor del daño es entre 100.000 y 1 millón de euros.
4 - 5	Muy dañino	Puede paralizar o repercutir en áreas de negocio. Valor del daño superior a 1 millón de euros. Puede haber muertes. Graves daños en la imagen.
5-7	Catastrófico	Puede hacer desaparecer la empresa.

5.3.4. Cuantificación del riesgo : Módulo del Vector Riesgo

Cálculo del riesgo en función de la probabilidad y del daño.

Una vez valorada la probabilidad y el daño, el proceso de cálculo del riesgo finaliza con su cuantificación.

El valor del riesgo es función de la probabilidad y del daño, cuya expresión matemática, quedó establecida como:

$$\mathbf{R\ f\ (P, D) = \sqrt{(P^2 + D^2)}.}$$

Aplicando ahora los intervalos de probabilidad y daño, de acuerdo con los parámetros obtenidos, la expresión matemática queda:

$$\mathbf{Ri = f\ (P\ 0{,}1\text{-}7, D1\text{-}5) = \sqrt{(P^2 + D^2)}.}$$

Obteniendo que el valor de un riesgo i (Ri) es función de la probabilidad (P) y el daño (D), para valores de probabilidad desde 0,1 hasta 7 y para valores del daño desde 1 hasta 7. Siendo esta función la raíz cuadrada de la suma de los cuadrados de ambos factores

Cálculo del riesgo en función de la frecuencia y de la vulnerabilidad.

Si en la expresión anterior sustituimos la probabilidad por su función tendríamos:

$$\boldsymbol{Ri = f\ ((F0{,}1\text{-}5\ ,\ V0{,}1\text{-}5), D)) = \sqrt{(\sqrt{(F^2 + V^2)})^2 + D^2} = \sqrt{(F^2 + V^2 + D^2)}}$$

El valor del riesgo será la raíz cuadrada de la suma de los cuadrados de los valores obtenidos para la frecuencia, la vulnerabilidad y el daño.

Parametrización y clasificación del Riesgo. Propuestas para su posible tratamiento.

La evaluación del riesgo es el proceso que consiste en comparar el riesgo calculado con ciertos criterios de riesgos para determinar su importancia[49].

Con el modelo para valorar el riesgo que se ha enunciado, el intervalo de posibles valores para éste será variable en función de los parámetros que consideremos. Si el evaluador decide cambiar los valores de cualquiera de los parámetros considerados o añadir otros factores, deberá componer sus propias tablas de valoración y evaluación.

Partiendo de los intervalos de posibles valores para cada parámetro:

P [0,1- 7]; F [0,1- 5] ; V [0,1- 5]; M [0,1- 3] ; Z [0,1- 4]

D [1- 7] ; C [0,7- 3] ; I [0,7- 4]

El valor del riesgo estará en el intervalo R [1 – 8,6]

Agrupando los posibles valores en intervalos de riesgo, tenemos:

- **1 - 2,8. Riesgo Trivial. (RTr):** Se trata de riesgos cuya probabilidad de suceder es muy baja y si sucediese, el daño que causaría sería mínimo. Se trata de riesgos asumibles.

[49] Definición de la Guía ISO /CEI 73 ya citada.

Pautas para el tratamiento:

La implantación de medidas para eliminarlo o reducirlo o su transferencia, se llevará a cabo si no precisan recursos importantes.

- **2,8 – 4,25. Riesgo Tolerable (RT):** Se trata de riesgos con alguna posibilidad de aparecer, ya se conoce algún caso (incluso ajenos a la propia empresa) en los que ha sucedido o aun siendo de remota aparición puede provocar un daño de cierta entidad, afectando a la Unidad, oficina o a la imagen.

  Pautas para el tratamiento:

  Tras valorar el coste del daño y de las posibles medidas se decidirá la adopción de éstas o su transferencia. No es urgente la adopción de medidas pudiendo abordarse a largo plazo o cuando las circunstancias lo permitan.

- **4,25 – 6,4. Riesgo Importante (RI):** Se trata de riesgos bastante dañinos, que pueden poner en peligro la actividad de un área y paralizar durante un tiempo una parte del negocio, o en los que el coste del daño es superior a 100.000 euros, aun considerando que su probabilidad es muy baja porque no se tiene conocimiento de que haya sucedido en alguna ocasión. También se tratará de riesgos importantes, los dañinos (que pueden provocar un daño de cierta entidad, afectando a la Unidad, oficina o a la imagen o de coste superior a 10.000 euros) de probabilidad media, es decir que ya han ocurrido en alguna ocasión.

  Pautas para el tratamiento:

  Los riesgos importantes no son asumibles con carácter general. En función de los costes del daño, de las medidas y del aseguramiento, se decidirá su tratamiento. El tratamiento debe abordarse a medio plazo, aun exigiendo recursos específicos.

- **6,4 - 8,2. Riesgo Grave (RG):** Se trata de riesgos muy dañinos, que pueden llegar a paralizar áreas de negocio, o causar graves daños a la imagen o cuyo coste es superior a 100.000 euros; incluso si su posible aparición es muy baja (no se conoce que haya sucedido nunca). También se consideran riesgos graves los bastante dañinos de probabilidad baja (porque se sabe que han sucedido alguna vez, no en la propia empresa), los dañinos de probabilidad media (que ya han sucedido en la empresa) incluso los banales (de escaso daño) con una probabilidad de manifestarse muy alta.

  Pautas para el tratamiento:

  Los riesgos graves no pueden asumirse. Será necesario adoptar medidas a corto plazo. Se transferirán además en todo o en parte.

- **8,2 - 10. Riesgo Intolerable (RIt):** Son riesgos muy dañinos, los que más daño pueden hacer, de bastante probable aparición (alta) ya que ha sucedió varias veces en la empresa o incluso de muy alta probabilidad.

  No pueden asumirse. Es muy urgente la adopción de medidas para eliminarlo. Serán necesarios planes de continuidad de negocio.

  Pautas para el tratamiento:

  Los riesgos intolerables no pueden asumirse, es urgente la adopción de medidas para eliminarlos o reducirlos. Es necesario también su transferencia y la adopción de planes de continuidad de negocio.

5.4. Modelo de mapa de riesgos obtenido aplicando el método vectorial.

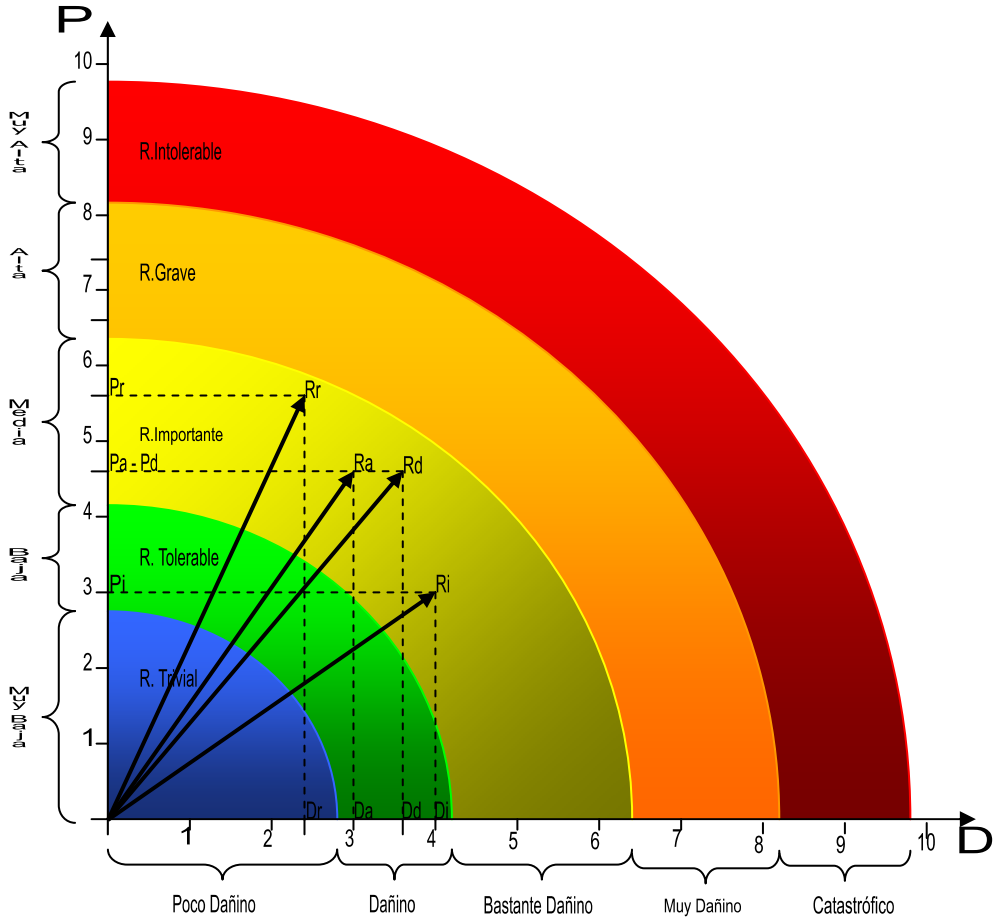


Fig. 9. Mapa de riesgos obtenido con el método vectorial.

Fuente: Elaboración Propia

Se trata de representar gráficamente el conjunto de todos los riesgos identificados en una empresa, organización o instalación, tras aplicar la fórmula establecida para el riesgo

Esta función permite la representación vectorial del riesgo, relacionando su posición relativa en un eje de abscisas y ordenadas (Probabilidad y Daño) con la cuantía del riesgo; siendo ésta el módulo del vector con origen el eje de condenas y extremo el punto (Pi, Di).

Así, mediante la concepción vectorial del riesgo, en función de su valor o módulo del vector, se pueden distribuir en anillos o intervalos de riesgo concéntricos, con centro en el origen de coordenadas. El intervalo de radio de cada uno coincide con los valores mínimo y máximo

posibles del riesgo para ese intervalo de clasificación. Se determinará por la organización en función de su política y aptitud ante los riesgos.

Como ya se ha dicho, en este mapa se refleja la dirección del vector riesgo, que viene dada por el ángulo ∂, indicando la relación entre probabilidad y daño o intensidad. Así, dentro de cada anillo la mayor o menor amplitud de este ángulo, indicará prevalencia de la probabilidad frente al daño o viceversa. Gráficamente se representa mediante la diferente tonalidad del color de cada anillo.

La organización puede contar con este tipo de mapa con una idea clara, concisa y rápida del riesgo, tanto en lo referente a su cuantía como en lo que atañe a la prevalencia de su carácter dañino o del probable.

Por todo lo expuesto, esta representación va a permitir visualizar los riesgos en su conjunto, con una idea rápida y precisa del valor de cada uno así como de la probabilidad de que suceda y del daño que ocasionaría.

5.5. Análisis de resultados.

Aplicación práctica de la nueva metodología. Consideración del caso propuesto

Consideremos nuevamente el caso tipo, ficticio, al que aplicamos experimentalmente los métodos de evaluación analizados en el Capítulo 3**.** Lo recordamos para facilitar su aplicación del método vectorial.

"Se trata de un recinto fabril, que alberga maquinaria de valor estimable, y difícil reposición. Consta de una nave con puerta normal de chapa. No dispone de ninguna medida de seguridad. Como medio de protección contra incendios sólo cuenta con extintores. La nave se encuentra en una parcela protegida por una valla de obra muy deteriorada, que no impide el paso. No hay ningún tipo de control de accesos. En la parcela se encuentra un depósito de combustible sin protección ninguna y en el que se aprecia una fuga de combustible. Este recinto se encuentra en un polígono dentro de una zona socialmente conflictiva. En el último año se han producido tres intrusiones en el interior de la fábrica, con robos de objetos varios en dos ocasiones, provocando en una de ellas la parada de la máquina principal por los daños ocasionados. El acceso por ajenos no autorizados a la parcela es muy frecuente."

En el supuesto planteado se identifican los siguientes riesgos:

- *Riesgo de incendio.*
- *Riesgo de robo.*
- *Riesgo de daños.*[50]
- *Riesgo medio ambiental por vertido de combustible.*

[50] Se adopta la denominación de "riesgo de daños" con la finalidad de contribuir al estudio, sin tipificar el daño como definición del riesgo. A estos efectos, consideramos "Riesgo de Daños" como el daño ocasionado en al fábrica de nuestro caso, ocasionado sin otra finalidad.

Valoración de los riesgos identificados en el caso propuesto mediante la aplicación del Método Vectorial de Evaluación.

Aplicando el Método vectorial, se obtienen los resultados que se recogen en la Tabla N. 8

RIESGO	VALOR DE LOS CRITERIOS				Cuantificación Del riesgo (ER) $R = \sqrt{F^2 + V^2 + D^2}$	Clase de riesgo
	Frecuencia Fr	Vulnerabidad V	Probabilidad P	Daño D		
Incendio	1,5 (no ha ocurrido en la empresa, si en otras)	Media 2,5	2,91 Baja	Muy Dañino 4	4,94	Riesgo Importante
Robo	4 (ha ocurrido varias veces)	Alta 4	5,65 Alta	dañino 2,5	6,17	Riesgo Importante (casi grave)
Daños	2,5 (ha ocurrido en una ocasión)	Alta 4	4,71 Media	Bastante dañino 3,5	5,86	Riesgo Importante
Medio Ambiental	2,5 (Ha ocurrido en una ocasión)	Alta 4	4,71 Media	Bastante dañino 3	5,02	Riesgo Importante

Tratamiento que Precisan los Riesgos, de acuerdo con el Método Vectorial de Evaluación.

Tras aplicar el método al caso propuesto se han obtenido los resultados de riesgo que Figuran en la tabla anterior.

Aplicando el tratamiento que Figura en la tabla para clasificar el riesgo, tendríamos, *Tabla N. 9*:

Riesgo	Clasificación	Tratamiento
Incendio	Importante	No asumible. Tratamiento a medio plazo Medidas y transferencia
Robo	Importante (casi grave)	No asumible. Tratamiento a corto plazo. Transferencia.
Daños	Importante	No asumible. Tratamiento a medio plazo Medida y transferencia
Ambiental	Importante	Tratamiento a medio plazo Tratamiento a medio plazo Medidas de control

5.6. Análisis crítico de la metodología vectorial de evaluación de riesgos de seguridad y medio ambiente.

A. Aplicabilidad del método.

- No se ha detectado dificultad para aplicar ninguno de los criterios propuestos a los cuatro riesgos identificados.

- Los parámetros de clasificación se ajustan a la realidad.

- Ofrece un amplio catálogo de criterios, de forma que cualquier riesgo se puede encuadrar en alguno sin caer en el criterio subjetivo del evaluador o reduciéndolo en gran parte.

- Este método se ha podido aplicar a todos los riesgos identificados, incluso al riesgo ambiental provocado por el vertido de combustible. No obstante, hay que matizar que tanto en este caso como en el de incendio, debe servir para tomar las primeras medidas y poner de manifiesto la necesidad de evaluaciones específicas que, por ejemplo valoren en qué medida ha podido dañar el medio ambiente ese vertido.

- La clasificación del riesgo se efectúa mediante conceptos, más que mediante cuantías, lo que permite su aplicabilidad, en principio, a todas las organizaciones.

B. Grado de objetividad.

- Los parámetros para incluir los factores o criterios considerados en la valoración están basados en hechos, incluyendo escasas indefiniciones, lo que reduce la carga subjetiva.

C. Fiabilidad de los resultados obtenidos

- Los grupos de clasificación no tienen una gran amplitud lo que posibilita al evaluador la inclusión en uno u otro grupo sin necesidad de utilizar su criterio, como único exponente.

- Al no tratarse de grupos de clasificación amplios, posibilita discriminar entre los mismos a los diferentes riesgos.

- En el caso de referencia, los resultados obtenidos para los riesgos identificados son acordes con la apreciación cualitativa. Así se califican todos como importantes, matizando que el robo (que ya ha sucedido varias veces) llega casi a grave. No se aprecian riesgos ni muy pequeños (tolerables o triviales) ni tan grandes que pongan en peligro incluso la continuidad de la fábrica.

D. Alcance del método de evaluación.

- Este método comprende todas las fases de la evaluación, da pautas para la identificación y el análisis y llega hasta una propuesta de tratamiento.

E. Posibilidad de representación gráfica.

- Reduce todos los factores a dos, probabilidad y daño o consecuencia, por lo que puede ser representado en un eje de coordenadas.

- Presenta como novedad que la representación del riesgo es en función del valor de su distancia al punto origen (el del vector), lo que permite aplicar idénticos tratamientos a riesgos de idéntico valor. Posibilitando un mapa de riesgos en función de este criterio.

- La dirección del vector riesgo, expresada por el ángulo que forma con el eje de ordenadas, se presenta como la relación de la probabilidad con la intensidad. Apreciación muy útil para decidir ante riesgos de igual valor.

CAPÍTULO 6. DISEÑO DE UNA METODOLOGÍA MIXTA POR PUNTOS, PARA IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS DE SEGURIDAD Y MEDIO AMBIENTE.

6.1. Justificación de un sistema de evaluación mixto por puntos.

El Método Vectorial para Evaluación de los Riesgos de Seguridad y Medio Ambiente, presenta el inconveniente de la necesaria parametrización previa de los factores de riesgo. Esta circunstancia limita en la práctica su aplicación en la medida en que se pretenda variar la relación de factores de riesgo a considerar. Hecho con el que nos encontraremos en la medida en que sea necesario disponer de un número elevado de evaluaciones, aplicadas sobre un variado elenco de activos.

Se ha definido la fase de identificación de riesgos como el punto de partida de la gestión directa del riesgo, como herramienta fundamental debe contarse con una buena check list que sistematice la recogida de datos. Durante esta fase, ante la gran cantidad de información que puede, y debe, recabarse, se necesita una herramienta potente para procesarla que automatice el proceso hasta la evaluación misma.

Así se ha concebido el Sistema de Evaluación Mixto por Puntos para Riesgos de Seguridad y Medio Ambiente.

Se dispone así de un método de evaluación eminente práctico, de aplicación directa y sencilla y preparado y concebido ya desde el diseño para ser informatizado.

Estas exigencias, además de las que se les han venido demandando a los otros métodos, implican también un sistema de valoración susceptible de llevar a resultados de forma rápida, precisa y con la menor carga subjetiva posible.

Así, el método que se presenta, más allá de un mero sistema de evaluación, se trata de una metodología que abarca gran parte del proceso de gerencia de riesgos, desde identificación muy detallada hasta el Mapa de Riesgos como producto de la evaluación.

El método de evaluación en cuestión, parte de la identificación exhaustiva de riesgos primarios o factores de riesgo en cada zona del edificio, asignándoles una valoración cualitativa prestablecida para cada uno. Para valorar los riesgos agregados o riesgos tipo que afectan a la instalación en su conjunto, se aplica un sistema de puntuación en función del valor cualitativo asignado a los riesgos primarios.

Cabe mencionar que el hecho de que se realizase mediante la aplicación directa de un número tan grande de preguntas muy precisas, unido a que el posible riesgo ya está prevalorado, reducen significativamente la carga subjetiva que pueda introducir cada evaluador.

6.2. Identificación de activos

No se puede entender ninguna referencia a los riesgos sin tener en cuenta los activos a los que afecta.

La metodología que se desarrolla se centra en la evaluación de los riesgos vinculados a la instalación. Considera, por tanto, los activos concretos, a los que su vinculación con las instalaciones pueda originarle algún daño, o de alguna forma, influir en que se produzcan.

Efectuar una identificación y valoración exhaustiva de los activos, escapa a las pretensiones de este método. Lo que no implica que no sea necesario para su aplicación tener una idea clara de los activos que pueden ser dañados por los riesgos objeto de la evaluación. Con este fin, ya la propia formulación de las preguntas está dirigida a identificar los riesgos de los activos concretos previamente considerados.

Por otra parte, en el test se incluyen preguntas destinadas directamente a identificar activos de valor importante, acreedores de riesgos específicos, previniendo que hayan podido quedar fuera de la identificación mediante el conjunto de las preguntas.

Cabe significar que la valoración exhaustiva y detallada de los activos, será necesaria para desarrollar otras fases de gerencia y para tomar la decisión sobre el tratamiento del riesgo.

6.3. Identificación de riesgos

En el método expuesto se opta por diferenciar, incluso documentalmente, la identificación del análisis, por las razones siguientes:

- Disponer de un documento de identificación diferenciado del análisis, permite descargar éste último de todo lo que no implica un riesgo relevante para la organización.

- El documento de identificación da una visión global y detallada de todas las circunstancias que afectan al edificio, recogiendo incluso situaciones de riesgo menor y riesgos controlados, considerando que podrían devenir en riesgos futuros si variasen las circunstancias actuales.

- El diseño diferenciado de identificación y análisis, permite abordar todo el proceso de gerencia de forma más estructurada y detallada.

6.3.1. Procedimiento para Identificación de Riesgos.

En esta fase se identificarán de forma metódica y exhaustiva todos los riesgos posibles, presentes y futuros así como las situaciones que puedan influir en los mismos.

Por un parte se recogerán datos de fuentes documentales y de las informaciones disponibles. Por otra, como fuente principal de información se recogerán los datos de campo mediante una

visita de inspección a la instalación o activo a evaluar. Los datos se volcarán en una check list específicamente diseñada.

Esta check list será la base para elaborar el análisis propiamente dicho y la posterior evaluación.

Recopilación de documentación e información.

Se trata de un proceso similar al descrito para el Método Vectorial, por lo que con el fin de no hacer tedioso el presente trabajo se remite a lo ya expuesto.

Conviene no obstante significar la necesidad de recopilar toda la información posible referente a la instalación que tenga relevancia para la Seguridad o en el Medio Ambiente.

6.3.2. La Check List para identificar los riesgos de seguridad y medio ambiente

Como herramienta para recoger los datos relevantes para el estudio del riesgo, se ha diseñado una check list específica para el ámbito de la Seguridad y el Medio Ambiente.

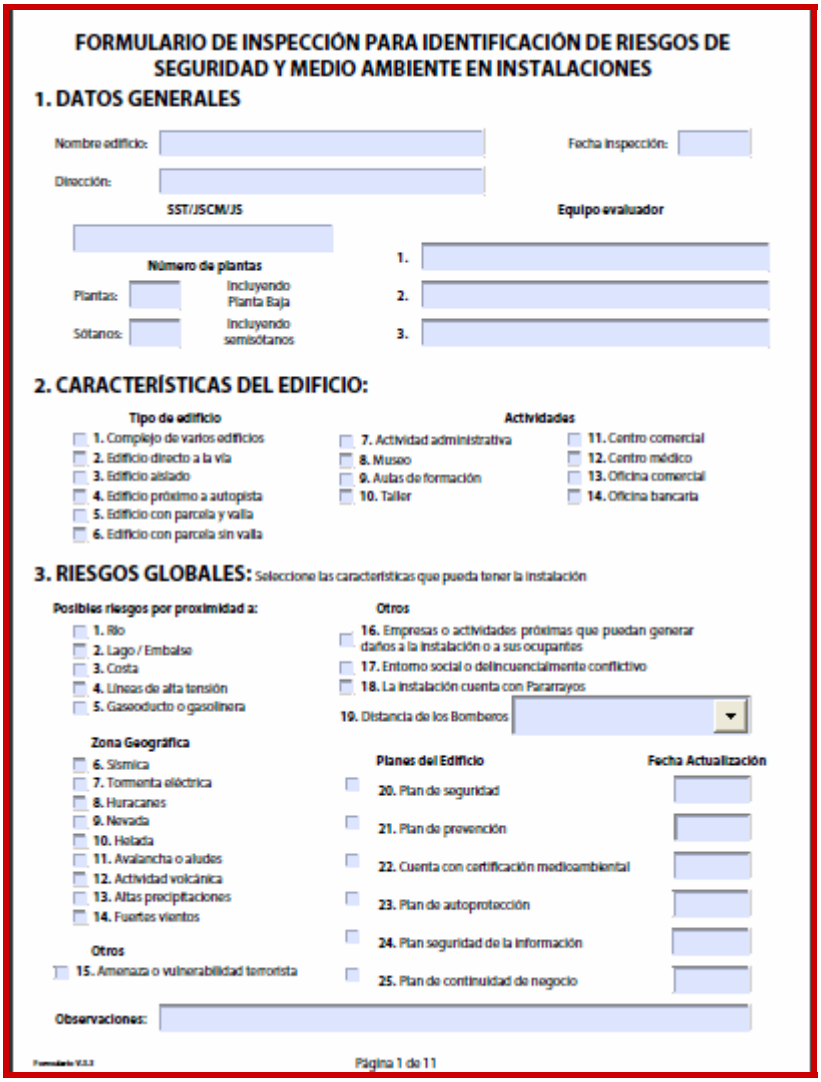
Esta check list se tratará mediante la aplicación informática adecuada, con el fin de obtener un elevado grado de disponibilidad de los datos, permitiendo su procesado posterior para elaborar el análisis. Debe resultar una herramienta de manejo sencillo, que pueda ser cumplimentada por cualquier usuario autorizado, pero impidiendo que se efectúen modificaciones en la configuración y estructura del Check List.

Las preguntas del Check List se dirigen a identificar los riesgos del ámbito de la Seguridad y el Medio Ambiente, que afectan o pueden provocar un daño a los activos de la empresa.

Para ello, a la hora de elaborar el Check List, se han considerado los activos vinculados y el catálogo o elenco de riesgos susceptible de dañarlos. Es necesario señalar que contar con un

catálogo de riesgos no puede constituir un límite a la hora de identificarlos. No puede suponer nunca una relación cerrada de riesgos, teniendo en cuenta que el universo de éstos es cambiante. Esto ha llevado a que el Check List se haya diseñado para identificar riesgos incluso no habituales.

La Check List se incluye como ANEXO II



FORMULARIO DE INSPECCIÓN PARA IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD Y MEDIO AMBIENTE EN INSTALACIONES

1. DATOS GENERALES

Nombre edificio: Fecha inspección:

Dirección:

SST/JSCM/JS

Equipo evaluador

1.

2.

3.

Número de plantas

Plantas: Incluyendo Planta Baja

Sótanos: Incluyendo semisótanos

2. CARACTERÍSTICAS DEL EDIFICIO:

Tipo de edificio

1. Complejo de varios edificios
2. Edificio directo a la vía
3. Edificio aislado
4. Edificio próximo a autopista
5. Edificio con parcela y valla
6. Edificio con parcela sin valla

Actividades

7. Actividad administrativa
8. Museo
9. Aulas de formación
10. Taller
11. Centro comercial
12. Centro médico
13. Oficina comercial
14. Oficina bancaria

3. RIESGOS GLOBALES: Seleccione las características que pueda tener la instalación

Posibles riesgos por proximidad a:

1. Río
2. Lago / Embalse
3. Costa
4. Líneas de alta tensión
5. Gaseoducto o gasolinera

Zona Geográfica

6. Sísmica
7. Tormenta eléctrica
8. Huracanes
9. Nevada
10. Helada
11. Avalancha o aludes
12. Actividad volcánica
13. Altas precipitaciones
14. Fuertes vientos

Otros

15. Amenaza o vulnerabilidad terrorista

Otros

16. Empresas o actividades próximas que puedan generar daños a la instalación o a sus ocupantes
17. Entorno social o delincuencialmente conflictivo
18. La instalación cuenta con Pararrayos
19. Distancia de los Bomberos

Planes del Edificio — Fecha Actualización

20. Plan de seguridad
21. Plan de prevención
22. Cuenta con certificación medioambiental
23. Plan de autoprotección
24. Plan seguridad de la información
25. Plan de continuidad de negocio

Observaciones:

Página 1 de 11

Fig. 10. Formulario para Inspección de Riesgos. Check List.

Fuente: Elaboración Propia

Características del Check List diseñada para identificar riesgos de Seguridad y Medio Ambiente.

Se trata de una batería de 531 preguntas dicotómicas, ante las que sólo cabe contestar sí ó no, marcando la respuesta cuando sea "sí", indicando esta respuesta positiva que existe la situación por la que se pregunta, sea dicha situación favorable a la aparición del riesgo o reductora del mismo.

Cada una de estas preguntas lleva a uno o varios riesgos tipo del catálogo. La presencia de riesgo puede deducirse bien porque existe la situación por la que se pregunta o bien porque no existe, dependiendo del sentido de la pregunta.

La Check List se ha estructurado en apartados con una batería de preguntas específicas para cada uno. Estos apartados se han definido mediante la agrupación de las posibles zonas de la instalación que albergan activos equivalentes en cuanto a naturaleza y valor y a las que afectan riesgos tipo similares. Circunstancias que han permitido homogeneizar los ítems.

La correcta aplicación del Check List parte de seleccionar los grupos de preguntas que son de aplicación, en función de las características y zonas de la instalación, debiendo marcarse las que sean de aplicación. La herramienta informática adecuada ignorará los grupos de preguntas no marcados.

Dentro del grupo de preguntas aplicable, dado que se ha concebido para varias zonas de naturaleza diferente, estandarizándolas, pueden encontrarse preguntas que no sean de aplicación al caso concreto. Ante esto se procederá respondiéndolas en el sentido que lleve a la ausencia de riesgo.

Si fuese necesario especificar a qué zonas concretas se refiere la situación observada, al final de cada grupo de preguntas se dispone de un campo para efectuar observaciones y aclaraciones.

Contenido y Estructuración del Check List

La Check List se estructura de la siguiente forma:

- **Datos identificativos.**

El documento recoge en primer lugar los datos identificativos del edificio y de los evaluadores. Datos, en principio, de escasa relevancia de cara al riesgo, pero necesarios.

- **Características del edificio.**

En este apartado se recogen las características del edificio y de la actividad que se desarrolla en el mismo, datos que pueden ser relevantes para el estudio del riesgo o que directamente pueden implicar un factor o fuente de riesgo.

- **Riesgos globales.**

Se identifican también los que se ha denominado como Riesgos Globales, incluyendo en éste apartado desde la existencia o no de amenaza terrorista, a la de riesgos de la naturaleza, de riesgos por el entorno socio económico, por proximidad a accidentes naturales, etc. Cabe mencionar que en este apartado se identifica también si dispone o no de planes de seguridad y medio ambiente, en toda su tipología. Se verifican asimismo circunstancias como la distancia a bomberos, mediante una pregunta con desplegable.

- **Por zonas de riesgo del edificio o instalación.**

Con la finalidad de hacer más operativa y manejable la herramienta, el grueso de las cuestiones se ha agrupado por zonas de la instalación que tienen un perfil de riesgo parecido.

Las preguntas formuladas para cada grupo se han particularizado para el mismo, intentando que se identifiquen la mayor parte de los aspectos que pueden indicar la existencia de riesgo.

Mediante un enfoque directo y preguntas dicotómicas y concatenadas, se ha pretendido reducir al máximo la carga subjetiva de las respuestas.

Los grupos por zonas de riesgo se han dispuesto siguiendo el orden lógico de la visita, por anillos y en profundidad. Así comienza con el vallado, parcela, y dependencias que se puedan encontrar en ésta, como el centro de control; continúa con la fachada y estructura, con el transformador si lo hubiera, con la oficina abierta al público, el parquin, si dispone de talleres, los cuartos técnicos (pese a que éstos se encontrarán, normalmente, en el parquin y en la zona de cubierta se tratan en el mismo grupo), zona de residuos, depósitos de combustible, almacenes cuartos de mantenimiento y de limpieza, fosa séptica y /o depuradora, archivos, sala de comunicaciones y /o CPD, hall, ascensores y escaleras, salidas de emergencia, cocina o cafetería, clínica o consulta médica, zona de correos, zonas de trabajo administrativo, salas de reuniones, de juntas o auditorios, despachos de dirección y despachos sensibles por el manejo de datos, y finalmente, patinillos.

- **Sistemas y medios de seguridad.**

Como otra agrupación de preguntas fuera del apartado de zonas de riesgo, ya que influyen en toda la instalación, se han dispuesto las relativas a los sistemas y medios de seguridad, con éstas se identifica si se dispone o no de los medios de todo tipo, que se consideran vitales para controlar los riesgos de Seguridad y Medio Ambiente, y si se encuentra en óptimo estado de funcionamiento.

- **Histórico de incidentes.**

Finalmente se ha habilitado otro apartado combinando campos y desplegables para recoger el histórico de incidentes, con sus consecuencias, riesgo asociado, fecha y gravedad.

Informatización y automatización del Check List

La herramienta informática, para elaborar el formato para recogida y almacenamiento de datos, que se ha aplicado en el modelo desarrollado ha sido la Suite de Adobe Acrobat 8 Professional 8.0, específicamente Adobe Live Cycle Designer 8.0.

Cabe no obstante utilizar cualquier otra herramienta que cumpla los requerimientos operativos que se han mencionado.

6.4. El análisis de riesgos

6.4.1. Concepto de Análisis de Riesgos

A partir de la información y datos obtenidos, se elaborará un documento de análisis de riesgos, en el que se recogerán los identificados que afecten a la instalación, a las personas o a las actividades, con sus causas, fuentes de riesgo y las vulnerabilidades detectadas; valorando la posibilidad de que se manifiesten y el daño a los activos, humanos y materiales.

6.4.2. El Catálogo de Riesgos

Se ha partido del catálogo de riesgos tipo que se ha identificado en el Capítulo 2 de este libro. Recordemos que en éste se recogen los riesgos probables para el conjunto de activos de una empresa, o que pueden afectar a su función, poniendo en riesgo la seguridad.

Este catálogo constituirá la guía de los riesgos tipo que probablemente afecten a los activos identificados en la instalación, sin que la identificación deba basarse exclusivamente en éstos, como si de una lista cerrada se tratase; ya que por la propia naturaleza cambiante de los riesgos, mediante la aplicación del Check List y el Análisis de Riesgos podrían detectarse otros no incluidos en ese catálogo y que no puedan descartarse.

Lo anterior lleva también a considerar que este proceso de identificación y análisis, además de su función principal en el proceso de gestión del riesgo, es una buena herramienta para mantener actualizado el catálogo de riesgos de la empresa u organización.

6.4.3. Riesgos Primarios o Fuentes de Riesgo y Riesgos Tipo

Para cada zona o activo de la instalación, mediante la aplicación de las preguntas correspondientes a ese grupo, se identificarán y analizarán los riesgos tipo del catálogo que le afecten. A estos riesgos identificados para zonas concretas se les denomina riesgos primarios.

El riesgo tipo se identificará y evaluará para el conjunto de toda la instalación y será en función de los riesgos primarios o fuentes de riesgo identificados en cada zona.

A modo de ejemplo, el riesgo de incumplimiento normativo por LOPD se analizará para zonas como el archivo, zona administrativa, etc., respondiendo al concepto de riesgos primarios de incumplimiento por LOPD. El riesgo tipo por incumplimiento de LOPD se valorará para toda la instalación y vendrá dado por la existencia de sus riesgos primarios en las diferentes zonas.

Relación de Riesgos Tipo cuya identificación es posible mediante esta Check List: Catálogo de Riesgos.

A los efectos de este método la referencia al catálogo de riesgos ha de entenderse como hecha a todos los riesgos cuya identificación es posible mediante esta Check List.

6.4.4. Algoritmo para obtener el Análisis de Riesgos

La metodología diseñada pretende elaborar de forma automatizada el informe de análisis de riesgos, partiendo del Check List cumplimentada.

A la automatización se llega elaborando un algoritmo que asocie cada una de las cuestiones planteadas con todos los riesgos del catálogo a los que afecte.

Un extracto del algoritmo que relaciona las preguntas con cada uno de los riesgos del catálogo, se incluye como ANEXO III.

Mediante los ítems se identificará si existen o no factores de riesgo o riesgos primarios, que afectan a los activos que se encuentren en las zonas examinadas o que puedan operar como factores de riesgo para el resto del edificio.

Como se ha indicado en lo referente al Check List, no se establece una correlación general, para todas las preguntas, entre la contestación en un sentido o en otro y la existencia de riesgo. Para establecer la existencia o no del riesgo, se considera el sentido de la pregunta; así, hay preguntas de cuya contestación afirmativa se deduce el riesgo, mientras que para otras es la contestación negativa la que indica la existencia de riesgo.

Se ha preferido este sistema, pese a ser su informatización más laboriosa, en lugar de optar por formular todas las preguntas en positivo o en negativo, dado que ese sistema implica dudas e induce a errores de interpretación para el evaluador que lo aplica.

La relación Ítem- riego, se materializa editando un texto prestablecido que ponga de manifiesto el riesgo derivado de la situación detectada.

Los grupos de preguntas que no se hayan marcado en el Check List, no se considerarán en el Análisis.

Las preguntas incluidas en los grupos aplicables, que no afecten, se habrán marcado o no en e el Check List de modo que no lleven a ninguna situación de riesgo.

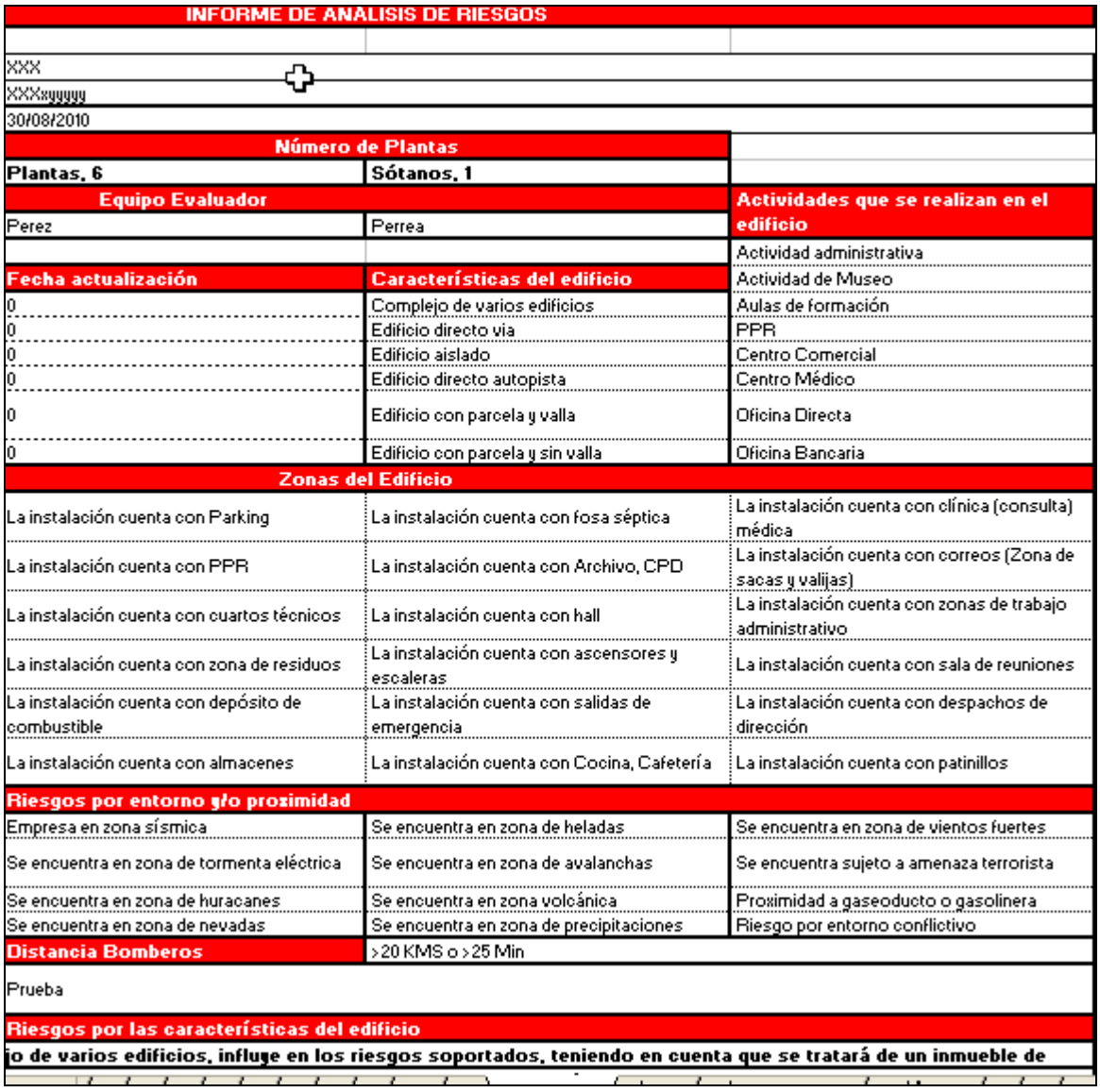
Recogida de las características generales del edificio, y de los posibles riesgos globales en el informe de riesgos.

Como se describió en el apartado de la estructura, desde el Check List se identifican situaciones y características del edificio y del entorno geográfico, que pueden tener una

influencia importante en los riesgos soportados. Se trata de circunstancias que no pueden asociarse a una zona del edificio ni a un riesgo concreto y cuya eliminación en origen implica medidas de gran calado, como el traslado del propio edificio o la eliminación de actividades o usos; acciones que, por su entidad e influencia en el negocio, difícilmente se acometerán. Por este motivo, se optará preferiblemente por mitigar o prevenir sus posibles efectos dañinos.

Pensemos, por ejemplo, en los riesgos derivados de que el edificio se encuentre en una zona con un grado importante de delincuencia o sujeta a riesgos de la naturaleza. Para evitar estas situaciones de riesgo habrá que considerar el traslado del propio edificio a otra zona, lo que puede ser muy problemático y desaconsejable. Habrá que optar por tanto por otro tipo de acciones para que la delincuencia de la zona tenga la menor incidencia posible en el desarrollo normal de la actividad del edificio y del propio negocio, por ejemplo incrementando las medidas de seguridad. De igual modo si se trata de una zona afectada por un riesgo de la naturaleza, antes que el traslado del edificio, se optará por planes de continuidad del negocio y medidas para minimizar los efectos.

Pese a su difícil valoración, resulta evidente que este tipo de situaciones debe recogerse en el análisis. Con este fin, partiendo de su identificación en el Check List, en el informe del análisis se recogerán unos textos ad hoc para cada posible situación, que pone de manifiesto la relevancia de cara al riesgo de esa situación.



INFORME DE ANALISIS DE RIESGOS		
XXX		
XXXxyyyyy		
30/08/2010		
Número de Plantas		
Plantas, 6	**Sótanos, 1**	
Equipo Evaluador		**Actividades que se realizan en el edificio**
Perez	Perrea	
		Actividad administrativa
Fecha actualización	**Características del edificio**	Actividad de Museo
0	Complejo de varios edificios	Aulas de formación
0	Edificio directo via	PPR
0	Edificio aislado	Centro Comercial
0	Edificio directo autopista	Centro Médico
0	Edificio con parcela y valla	Oficina Directa
0	Edificio con parcela y sin valla	Oficina Bancaria
Zonas del Edificio		
La instalación cuenta con Parking	La instalación cuenta con fosa séptica	La instalación cuenta con clínica (consulta) médica
La instalación cuenta con PPR	La instalación cuenta con Archivo, CPD	La instalación cuenta con correos (Zona de sacas y valijas)
La instalación cuenta con cuartos técnicos	La instalación cuenta con hall	La instalación cuenta con zonas de trabajo administrativo
La instalación cuenta con zona de residuos	La instalación cuenta con ascensores y escaleras	La instalación cuenta con sala de reuniones
La instalación cuenta con depósito de combustible	La instalación cuenta con salidas de emergencia	La instalación cuenta con despachos de dirección
La instalación cuenta con almacenes	La instalación cuenta con Cocina, Cafetería	La instalación cuenta con patinillos
Riesgos por entorno y/o proximidad		
Empresa en zona sísmica	Se encuentra en zona de heladas	Se encuentra en zona de vientos fuertes
Se encuentra en zona de tormenta eléctrica	Se encuentra en zona de avalanchas	Se encuentra sujeto a amenaza terrorista
Se encuentra en zona de huracanes	Se encuentra en zona volcánica	Proximidad a gaseoducto o gasolinera
Se encuentra en zona de nevadas	Se encuentra en zona de precipitaciones	Riesgo por entorno conflictivo
Distancia Bomberos	>20 KMS o >25 Min	
Prueba		
Riesgos por las características del edificio		
io de varios edificios, influye en los riesgos soportados, teniendo en cuenta que se tratará de un inmueble de		

Fig. 11. Ejemplo del análisis de riesgos obtenido tras el tratamiento informático del Check List y la aplicación del algoritmo. Fuente: Elaboración propia.

6.4.5. Valoración cualitativa.

En el análisis de riesgos se recogerá una primera valoración cualitativa de todos los riesgos primarios o factores de riesgo que se han detectado con todas y cada una de las preguntas formuladas.

Para llegar a la valoración de cada riesgo tipo, previamente se ha procedido a valorar todos los riesgos primarios, cuya identificación se posibilita mediante el Check List, como alto, medio o bajo.

Así, cuando la respuesta a las preguntas lleve a la existencia del riesgo, el algoritmo aplicado, también llevará a clasificarlo como alto, medio o bajo.

Con este sistema de valoración cualitativa, se integran tanto aspectos probabilísticas como de impacto o intensidad.

Cada una de estas gradaciones responde al siguiente criterio:

Riesgo Alto: Equivale a un riesgo grave, se tratará de un riesgo de probable o muy probable manifestación y que además causará un impacto importante.

Debe ser corregido o controlado de forma prioritaria e inmediata, destinando los recursos necesarios para ello

Riesgo Medio: Se tratará de un riesgo moderado, bien porque su probabilidad no es elevada o bien porque aún siendo ésta elevada, el impacto no sería importante.

Deben corregirse a medio plazo, para ello se tendrán en cuenta los recursos disponibles y razones de oportunidad.

Riesgo Bajo: Se tratará en cualquier caso de un riesgo posible y susceptible de provocar un daño, evidentemente, la ausencia de cualquiera de estos dos componentes indicaría la inexistencia del riesgo, lo que no se consideraría a efectos del análisis. Se tratará de un riesgo poco probable y cuyo impacto tampoco sería muy significativo.

Con este sistema de valoración prestablecido de forma genérica, el usuario que cumplimenta el Check List valorará el riesgo directamente, ya que la valoración está prestablecida y se extrae automáticamente en el análisis a partir de la contestación misma a la pregunta. Se reduce así la carga subjetiva que pueda introducir el analista, al tiempo que se unifican los criterios.

No obstante el analista tiene la posibilidad de variar la calificación de determinados riesgos identificados, en aquellos casos en la calificación establecida con carácter general, claramente, no se corresponda con la realidad.

Cuando el analista varié la calificación del riesgo prestablecida, deberá justificarlo en las observaciones del documento del análisis.

Ver el ANEXO III, en cuanto al Algoritmo que incluye también la valoración cualitativa de cada posible riesgo.

6.4.6. Informe final de Análisis de Riesgos.

Partiendo de la cumplimentación del Check List, mediante la aplicación informática adecuada, se editará un informe de Análisis de Riesgos que contendrá:

- Los datos identificativos del edificio y de los evaluadores.
- La existencia o no de planes y protocolos de Seguridad y Medio Ambiente y los riesgos asociados a las posibles carencias, con su valoración como alto, medio o bajo.
- Los riesgos derivados de las características, actividad y situación que afectan de manera global a todo la instalación, incluyendo su valoración.
- Identificación de las características del edificio o de la zona que pueden modificara la situación de riesgo, incluyendo un análisis genérico sobre dicha influencia.
- Los riesgos primarios asociados a cada situación detectada, clasificados por grupos y zonas, asociados a la causa y vulnerabilidad detectada e incluyendo la valoración cualitativa para todos y cada uno. Se recogen también las observaciones aclaratorias.
- La situación y riesgos derivados de los sistemas y medios de Seguridad. Valorando cada uno.

Se incluye como ANEXO IV un extracto del modelo de Informe de Análisis de Riesgos.

3.0.	Riesgos del entorno (riesgos globales)		
Riesgo	**Alto**	**Medio**	**Bajo**
Normativo de Medio Ambiente		No existe certificación medioambiental	
Normativo Autoprotección (Incendios)	No existe plan de autoprotección		
Normativo (otras causas)		No existe plan de continuidad de negocio	No existe plan de prevención
Daños, posible RC			No existe plan de autoprotección
			No existe plan de prevención
Incendio		No existe plan de autoprotección	Proximidad a gaseoducto o gasolinera
			Se encuentra en zona de tormenta eléctrica
			Se encuentra en zona volcánica
			Se encuentra en zona de huracanes
			Empresa en zona sísmica
			Riesgo por empresas colindantes
Riesgo de la información	No existe plan de continuidad de negocio	No existe plan de seguridad	Riesgo por entorno conflictivo
	No existe plan de seguridad de la información		
Imagen		No existe certificación medioambiental	No existe plan de seguridad de la información
			No existe plan de autoprotección
Riesgos de la naturaleza	Empresa en zona sísmica	Proximidad a ríos	Proximidad a lagos
	Se encuentra en zona de huracanes	Se encuentra en zona de vientos fuertes	Proximidad a costa
	Se encuentra en zona de avalanchas	Se encuentra en zona de precipitaciones	
	Se encuentra en zona volcánica	Se encuentra en zona de tormenta eléctrica	
		Riesgo por no tener parrarayos	
		Se encuentra en zona de nevadas	
		Se encuentra en zona de heladas	
Químicos (explosión)		Proximidad a gaseoducto o gasolinera	Riesgo por empresas colindantes
Físicos (Eléctrico)			Proximidad líneas de alta tensión
Medio ambientales		No existe certificación medioambiental	Proximidad a ríos
		Proximidad a gaseoducto o gasolinera	Proximidad a lagos
			Proximidad a costa
			Riesgo por empresas colindantes
Intrusión		Riesgo por entorno conflictivo	No existe plan de seguridad de la información
		No existe plan de seguridad	
Terrorismo	Se encuentra sujeto a amenaza terrorista		No existe plan de seguridad

Fig.12 . Informe de Análisis de Riesgos. Ejemplo de riesgos de zonas, con valoración.

Fuente elaboración propia

6.4.7. Automatización e informatización del proceso.

Aplicando la **herramienta informática adecuada**, se automatizará el proceso de forma que el marcado o no de las preguntas planteadas lleve a la edición del texto indicando el riesgo de que se trata con la correspondiente valoración cualitativa, no considerando los grupos de preguntas que no aplican.

En el caso que se ha puesto en práctica se ha utilizado la herramienta informática ya descrita, que permite extraer los informes en EXCELL, evitando la manipulación no autorizada del algoritmo o del Check List.

6.4.8. Diferencia entre evaluación y análisis de riesgos: La evaluación cualitativa como alternativa a la cuantificación del riesgo.

Valoración cualitativa.

En el análisis de riesgos se recogerá una primera valoración cualitativa de todos los riesgos primarios o factores de riesgo que se han detectado con todas y cada una de las preguntas formuladas.

Para llegar a la valoración de cada riesgo tipo, previamente se ha procedido a valorar todos los riesgos primarios, cuya identificación se posibilita mediante el Check List, como alto, medio o bajo.

Así, cuando la respuesta a las preguntas lleve a la existencia del riesgo, el algoritmo aplicado, también llevará a clasificarlo como alto, medio o bajo.

Con este sistema de valoración cualitativa, se integran tanto aspectos probabilísticas como de impacto o intensidad.

Cada una de estas gradaciones responde al siguiente criterio:

Riesgo Alto: Equivale a un riesgo grave, se tratará de un riesgo de probable o muy probable manifestación y que además causará un impacto importante.

Debe ser corregido o controlado de forma prioritaria e inmediata, destinando los recursos necesarios para ello

Riesgo Medio: Se tratará de un riesgo moderado, bien porque su probabilidad no es elevada o bien porque aún siendo ésta elevada, el impacto no sería importante.

Deben corregirse a medio plazo, para ello se tendrán en cuenta los recursos disponibles y razones de oportunidad.

Riesgo Bajo: Se tratará en cualquier caso de un riesgo posible y susceptible de provocar un daño, evidentemente, la ausencia de cualquiera de estos dos componentes indicaría la inexistencia del riesgo, lo que no se consideraría a efectos del análisis. Se tratará de un riesgo poco probable y cuyo impacto tampoco sería muy significativo.

Con este sistema de valoración prestablecida de forma genérica, el usuario que cumplimenta el Check List valorará el riesgo directamente, ya que la valoración está prestablecida y se extrae automáticamente en el análisis a partir de la contestación misma a la pregunta. Se reduce así la carga subjetiva que pueda introducir el analista, al tiempo que se unifican los criterios.

No obstante el analista tiene la posibilidad de variar la calificación de determinados riesgos identificados, en aquellos casos en la calificación establecida con carácter general, claramente, no se corresponda con la realidad.

Cuando el analista varié la calificación del riesgo prestablecida, deberá justificarlo en las observaciones del documento del análisis.

Ver el ANEXO III, en cuanto al Algoritmo que incluye también la valoración cualitativa de cada posible riesgo.

6.5. La evaluación de riesgos

Mediante la metodología específica para evaluar los riesgos de seguridad y medio ambiente, que se expone a continuación, se pretende cuantificar los riesgos con la menor carga subjetiva posible, integrando el mayor número de factores que lleven o incidan en ese riesgo.

La información proporcionada por esta evaluación permitirá establecer prioridades de actuación, en función de criterios racionales, medibles y admitidos por la organización.

A partir de la cuantificación de los riesgos se abordará su representación gráfica, elaborando el mapa de riesgos del edificio.

La cuantificación prestablecida de todos y cada uno de los riesgos detectados, mediante la aplicación de los 531 ítems, ante los que sólo cabe contestar sí ó no, reduce de forma evidente la carga subjetiva.

6.5.1. Naturaleza del método de evaluación.

El método consistirá en la obtención de una puntuación para cada riesgo tipo, partiendo de la identificación y valoración cualitativa prestablecida para cada factor de riesgo o riesgo primario detectado en cada una de las zonas del edificio.

Se trata por tanto de una Metodología Mixta mediante un Sistema de Puntos.

6.5.2. Puntuación de los riesgos

El valor de cada riesgo tipo se obtendrá en función de las valoraciones cualitativas de los riesgos primarios o factores de riesgo de ese tipo que se hayan identificado, en relación con el número de ítems de las zonas aplicables.

Número de ítems aplicable a cada riesgo tipo y de ítems que lo han identificado.

Como se ha señalado para la Identificación y el Análisis, desde el Check List se seleccionan los grupos de preguntas que son aplicables a la instalación.

Mediante el algoritmo se relaciona cada ítem de los grupos seleccionados con todos los riesgos tipo a cuya identificación puede llevar. Además, cada uno de estos posibles riesgos detectados con las preguntas del Check List, se ha prevalorado como “alto”, “medio” o “bajo”. (Es decir, se trata de una evaluación cualitativa prestablecida para todos los posibles riesgos primarios).

Contestando a las preguntas contenidas en los grupos o zonas que sean de aplicación a la instalación, y por tanto se han debido seleccionar, se identificarán los riesgos concretos que le afecten, incluyendo su valoración cualitativa. A estos riesgos concretos que afectan a cada zona se les llama riesgos primarios. La integración de todos los riesgos primarios de la misma tipología lleva a los riesgos tipo (equivalente al riesgo agregado) para el conjunto de la instalación.

Lo anterior posibilita que para cada Riesgo Tipo del catálogo se obtenga:

o **El número de preguntas QUE PUEDEN LLEVAR A CADA UNO DE LOS RIESGOS, en sus diferentes grados.** De entre las que le son de aplicación a la instalación.

A los efectos de este método, denominaremos:

- Número máximo de ***cuestiones que pueden llevar a un Riesgo Tipo, i, en grado ALTO***:

RA $_i$

- Número máximo de ***cuestiones que pueden llevar a un Riesgo Tipo, i, en grado MEDIO***:

RM i

- Número máximo de ***cuestiones que pueden llevar a un Riesgo Tipo ,i, en grado BAJO***:

RB i

o **Número de preguntas que han IDENTIFICADO un factor de riesgo del tipo considerado en cada uno de sus diferentes grados.**

A los efectos de este método denominaremos:

- Número de ***preguntas que han identificado un Riesgo Tipo i, en grado ALTO***:

IRA i

- Número de **preguntas que han identificado un Riesgo Tipo i, en grado MEDIO**:

IRM i

- Número de **preguntas que han identificado un Riesgo Tipo i, en grado BAJO**:

IRB i

Puntuación posible para cada Riesgo Tipo.

El intervalo de puntuación que puede obtener cada riesgo tipo va de 0 a 10. Sin que en ningún caso se pueda obtener 0, que equivaldría a que no existe riesgo, (bien porque la probabilidad es cero o porque no provoca ningún daño). Si no existe riesgo, evidentemente, no cabe evaluación alguna.

La puntuación opera en sentido creciente del riesgo, es decir, a mayor puntuación más riesgo.

Así, una puntuación de 10 o próxima a esta puntuación, la máxima posible, indica que se trata de un riesgo muy importante y grave. Será un riesgo muy probable, casi cierto, y de consecuencias muy dañinas.

Puntuaciones inferiores a 5, indican un riesgo medio, y superiores riesgo alto.

Relación de la puntuación obtenida con la calificación del Riesgo Tipo

Un riesgo será alto si obtiene una puntuación mayor de 5. Será medio si obtiene entre 2 y 5, y bajo si obtiene de 0 a 2. Aplicando un criterio similar al utilizado para la valoración cualitativa de los riesgos primarios, pero ahora con las equivalencias numéricas una vez cuantificado el riesgo aplicando las reglas que se indicarán, se tiene:

- ✓ **Riesgo Tipo Alto:** Puntuación mayor o igual a cinco y menor que 10.

($5 \leq RA < 10$)

- ✓ **Riesgo Tipo Medio:** Puntuación menor a cinco y mayor o igual a 2

($2 \leq RM < 5$).

- ✓ **Riesgo Tipo Bajo:** Puntuación menor a 2 y mayor a 0.

(0 <RB <2).

Respondiendo cada una de estas gradaciones a lo siguiente:

Riesgo Tipo Alto: Equivale a un riesgo grave, se tratará de un riesgo de probable o muy probable manifestación y que además causará un impacto importante.

Debe ser corregido o controlado de forma prioritaria e inmediata, destinando los recursos necesarios para ello.

Corrigiendo los factores de riesgo primarios en grado alto, se corrige el riesgo tipo alto.

Riesgo Tipo Medio: Se tratará de un riesgo moderado, bien porque su probabilidad no es elevada o bien porque aun siendo ésta elevada, el impacto no sería importante.

Deben corregirse a medio plazo, para ello se tendrán en cuenta los recursos disponibles y razones de oportunidad.

Aun corrigiéndolos, en tanto en cuanto persista algún riesgo tipo alto, no se habrá logrado un control aceptable del riesgo.

Riesgo Tipo Bajo: Se tratará en cualquier caso de un riesgo posible y susceptible de provocar un daño, evidentemente, la ausencia de cualquiera de estos dos componentes indicaría la inexistencia del riesgo. Pero se tratará de un riesgo poco probable y cuyo impacto tampoco sería muy significativo.

También deben controlarse. En función de la apetencia de la empresa por el riesgo, los recursos y el coste, se decidirá la oportunidad para corregirlo.

Cálculo de la puntuación para cada Riesgo Tipo.

Para obtener la puntuación de cada riesgo tipo para toda la instalación, se parte de lo siguiente:

- Los riesgos primarios o factores de riesgo detectados en cada una de las zonas analizadas, van incrementando el valor del riesgo tipo.

- Como se ha visto, los riesgos identificados (primarios) se han clasificado, directamente a partir de la contestación de las preguntas del Check List, como altos, medios o bajos.

- El valor de cada Riesgo Tipo identificado para todo el edificio o instalación, dependerá de la calificación de los riesgos primarios de ese tipo que se han identificado y analizado para cada zona.

La valoración concreta de los riesgos se efectuará aplicando las ecuaciones que se desarrollan a continuación.

Valoración cuantitativa de los riesgos

Puntuación de los riesgos valorados cualitativamente como Altos.

Todos los riesgos primarios referentes a un mismo riesgo tipo, identificados y valorados en cada zona como Altos, puntúan en conjunto como 5.

Esto quiere decir que, en tanto en cuanto se haya identificado un factor de riesgo en grado alto, ese riesgo tipo concreto va tener siempre un valor de 5 o superior. En consecuencia implicará que se considere todo el riesgo como alto.

Por el contrario, si para un riesgo tipo no se ha identificado ningún factor de riesgo o riesgo primario de grado alto, nunca se alcanzará el 5 para ese riesgo tipo; lo que equivale a considerar que ese riesgo en ningún caso se considerará alto.

Puntuación de los riesgos valorados cualitativamente como Medios.

La puntuación que corresponde a cada riesgo primario calificado como medio, será la obtenida de prorratear 3 (valor del intervalo de 2 a 5) entre el número de ítems aplicables que podrían llevar riesgo medio.

Así el valor de cada riesgo primario identificado de grado medio será:

$$\mathbf{VRM\ i = (3 / RM\ i)}$$

Siendo RMi, el número máximo de ítems posibles que llevan a riesgo de grado medio.

El valor total de todos los riesgos primarios de grado medio correspondientes a un tipo concreto que se han identificado, se obtendrá multiplicando el valor de cada riesgo primario por el número de ítems que han identificado este riesgo en grado medio. :

$$\mathbf{VRM = (3 / RM\ i)\ X\ I\ RMi}$$

Siendo IRMi, el número de preguntas que han identificado riesgos primarios del **Riesgo Tipo$_i$ en grado medio.**

Puntuación de los riesgos valorados cualitativamente como Bajos

La puntuación que corresponde a cada riesgo primario calificado como bajo, será la obtenida de prorratear 2 (valor del intervalo de 0 a 2) entre el número de ítems aplicables que llevasen a riesgo bajo.

Así el valor de cada riesgo primario identificado de grado bajo será:

$$\mathit{VRB\ i = (2 / RBi)}$$

Siendo RBi, el número máximo de preguntas (o preguntas aplicables) que llevan a un determinado riesgo en grado bajo.

El valor total de todos los riesgos primarios de grado bajo correspondientes a un tipo concreto, que se han identificado, se obtendrá multiplicando el valor de cada riesgo primario por el número de ítems que han identificado este riesgo en grado medio:

$$\mathbf{VRB} = (2 / \mathbf{RBi}) \text{ X } \mathbf{IRBi} = \mathbf{2\ RBi\ /\ IRBi}$$

Siendo IRBi, el número de preguntas que han identificado riesgos primarios del riesgo tipo i, en grado bajo

Puntuación total del Riesgo Tipo o Riesgo Agregado para el conjunto de la Instalación.

El valor del riesgo tipo o agregado para toda al instalación, se obtendrá sumando el valor de los tres valores obtenidos para los riesgos primarios de grado riesgo alto, medio y bajo.

*Así**, el valor del Riesgo i,** será*:

$$VRi = VRM + VRB, \text{ para } IRA > 0.$$

$$Y$$

$$VRi = VRM + VRB + 5 \quad \text{Para } IRA = 0.$$

Es decir, el valor del riesgo tipo i, será la suma del valor de los Riesgos Medios más el valor de total de los Riesgos Bajos, si no existen Riesgos Altos o la suma del valor Total de los Riesgos Medios más el valor total de los Riesgos Bajos incrementado en cinco, si existe algún Riesgo Alto.

6.6. Informes de Riesgos

Con los riesgos evaluados, mediante la aplicación informática oportuna, se pueden extraer de forma fácil los informes de riesgos que se precisen.

Entre estos posibles informes, se consideran de vital importancia los siguientes:

- **Informe de Riesgos Tipo Altos.** Permitirá establecer la prioridad para la adopción de las medidas, centrándola en los riesgos más importantes que es preciso corregir de forma inmediata.
- **Informe de Riesgos Tipo Altos por zonas de la instalación.** Permitirá una visión de los riesgos altos por zonas, con el fin de facilitar la adopción de las medidas de control más urgentes en cada zona de la instalación.
- **Informe Completo de Riesgos para toda la Instalación.** Este informe permite una visión general de todos los riesgos. Complementa al Mapa de Riesgos.
- **Otros informes de riesgos.** Se podrán extraer de igual modo el informe de riesgos medios o el de riegos bajos, así como los informes por Riesgo Tipo; para tener una visión, por ejemplo de cómo está el riesgo de imagen en toda la instalación o el riesgo de incendio que se está soportando.

Como ANEXOS IV y V se incluyen ejemplos de Informes de Riesgos.

INFORME DE ANALISIS DE RIESGOS ALTOS POR RIESGO	
Nombre edificio:	XXX
Dirección	XXXxyyyyy
Fecha inspección	30/08/2010
Riesgo	Zona del edificio
Daños Posible RC	
Transformador	Los accesor al transformados no se controlan
Fosa Séptica / Depuradora	Es posible que una persona caiga en la fosa
Cocina / Cafetería	No se detectan las fugas en las cámaras frigoríficas
Cocina / Cafetería	Las cámaras frigoríficas no indican si alguien permanece dentro
Cocina / Cafetería	Se aprecian sustancias contaminantes o peligrosas
Cocina / Cafetería	No se realiza control de alimentos por sanidad
Sistemas y medios de seguridad	La instalación no cuenta con los seguros suficientes para riesgos de RC
Imagen	
Clínica, Consulta médica	Se aprecia suciedad y desorden
Trabajo Administrativo	En la OD se arrojan a la papelera documentos sensibles
Incendio	
Sala de contro y de seguridad	En el CC hay objetos o líquidos inflamables
Sala de contro y de seguridad	El CC no tiene protección contra incendios
Parcela	La parcela no tiene protección contra incendios
Transformador	Existen elementos que incrementan la carga de fuego
Transformador	El transformador no cuenta con protección contra incendios
Parking	Hay elementos suceptibles a provocar un incendio
Parking	No existe detección automática
Taller	No hay detección automática
Cuartos Técnicos	Se aprecian líquidos o productos inflamables
Cuartos Técnicos	No cuenta con detección automática
Depósito combustibles	Existen agentes próximos que puedan provocar la ignición
Depósito combustibles	No cuenta con detección automática
Depósito combustibles	Equipo contra incendio no adecuado a la carga de fuego
Depósito combustibles	No existe ó no se aplica protocolo para trabajos en caliente
Depósito combustibles	No está prohibido fumar en la zona
Sala de Comunicaciones CPD	Existen elementos que supongan incremento a la carga de fuego
Sala de Comunicaciones CPD	Se detectan productos inflamables
Sala de Comunicaciones CPD	No cuenta con detección automática de incendios
Sala de Comunicaciones CPD	Se detectan elementos que puedan provocar ignición
Sala de Comunicaciones CPD	No existe ó no se aplica protocolo para trabajos en caliente
Sala de Comunicaciones CPD	No está prohibido fumar en la zona
Hall	No existe protección contra incendios adecuada
Cocina / Cafetería	Se detectan productos inflamables
Cocina / Cafetería	No cuenta con detección automática de incendios
Cocina / Cafetería	No cuenta con extintores adecuados
Trabajo Administrativo	Se detectan productos inflamables
Trabajo Administrativo	No cuenta con detección automática de incendios
Sala de Reuniones	Existen elementos que supongan incremento a la carga de fuego
Sistemas y medios de seguridad	Las señales de incendio no se recepcionan a una central atendida permanentemente

Fig.13. Informe de Riesgos Tipo Altos clasificados por riesgo. Pág. 1.

Fuente Elaboración propia

6.7. Representación gráfica. Mapa de Riesgos

Disponiendo de la valoración de todos los riesgos tipo de una instalación, es posible representarlos gráficamente mediante un diagrama de barras.

En el eje de abscisas se marcará la valoración de cada riesgo de 0 a 9, y en el de ordenadas Figurará la relación de riesgos tipos presentes en la instalación o edificio.

El gráfico deberá resaltar las líneas correspondientes a los valores de riesgo que suponen el paso de una calificación a otra; así se marcará con una línea horizontal el valor 5, por debajo de la cual los riesgos serán altos y otra para el valor 8, marcando los medios.

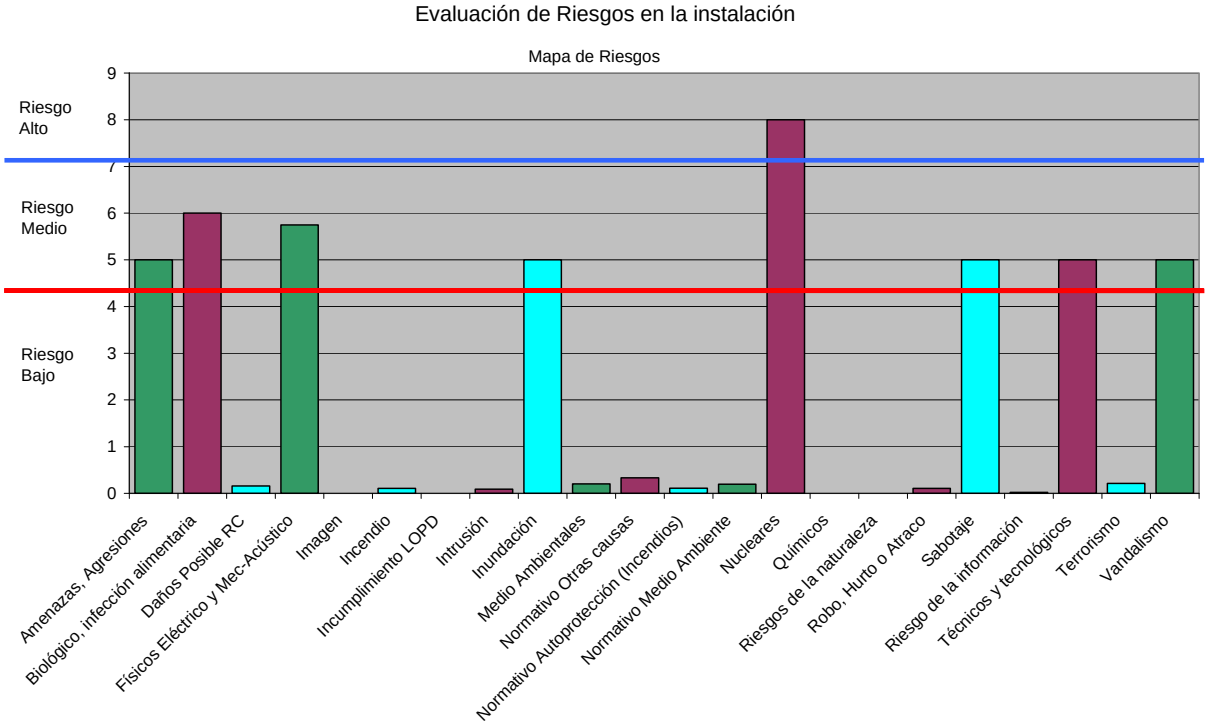


Fig. 14. Ejemplo de la Representación Gráfica o Mapa de Riesgos obtenido mediante esta evaluación. Fuente Elaboración Propia.

6.8. Sobre la herramienta informática necesaria

La herramienta que se precisa debe permitir la gestión del proceso en su totalidad, es decir:

- Deberá permitir la recogida de datos mediante el Check List de forma fácil y ágil. Posibilitando al usuario las modificaciones en cuanto a las marcaciones, pero restringiendo mediante perfiles el acceso a la modificación de los ítems o la estructura del cuestionario.
- Partiendo del Check List, y mediante la aplicación del algoritmo, deberá procesar la información emitiendo un Informe de Análisis de Riesgos por zonas y con la valoración cualitativa de los mismos. Los resultados de análisis automatizado podrán ser modificados por los expresamente autorizados (el Responsable de la Evaluación), descartando que el usuario que cumplimenta el Check List, si carece de los atributos correspondientes, pueda efectuar estas modificaciones.
- Mediante la aplicación de las ecuaciones para el cálculo de la puntuación de los riesgos tipo, la herramienta, automatizará la evaluación.
- Posibilitará la representación gráfica de los riesgos valorados y la emisión de los diferentes informes.

Como se ha indicado, este método, en todas sus fases, se ha desarrollado inicialmente con la aplicación de la Suite de Adobe Acrobat 8 Professional 8.0, específicamente Adobe Live Cycle Designer 8.0., herramienta que cumple gran parte de las expectativas.

No obstante, esta herramienta no permite su extensión total a usuarios que carezcan de este programa. Debiendo remitirse el Check List cumplimentada al evaluador que disponga del programa para que emita los informes y gráficas. Con el inconveniente añadido de que, si no se dispone del Acrobat 8 o superior, no se permite que el usuario almacene automáticamente el cuestionario cumplimentado en todo o en parte.

Por este motivo no se descartan otras herramientas que permitan universalizar la aplicación de esta metodología sin necesidad de un programa ad hoc.

CAPÍTULO 7. CONCLUSIONES.

La génesis de este trabajo hay que buscarla en varias ideas, todas ellas relacionadas con la labor cotidiana de un gerente de riesgos, con el decisivo condicionante de que su ámbito de riesgo se centre en los de seguridad y medio ambiente.

Un gerente de riesgos de seguridad puede encontrase con un panorama ciertamente desolador pero a la vez envuelto en un halo de esperanza, lo que hace atractiva su labor. Aseveramos esto considerando que, como se ha puesto de manifiesto en este trabajo, el mundo de la gerencia y el mundo de la seguridad parecen tratarse de ámbitos ajenos y a la vez alejados. Pero a poco que se analice la situación se vislumbran más factores de coincidencia que de alejamiento.

No en vano, estos dos ámbitos, junto al resto de ámbitos de riesgo tienen algo muy importante en común, lo esencial de su trabajo, esto es el RIESGO. Abordado, efectivamente desde ópticas distintas, incluso de naturaleza distinta, pero riesgo al fin y al cabo. Y como tal preocupa a la organización.

Decimos que el panorama también es esperanzador, no hay más que comprobar, como se extrae en esta obra,, que las líneas de trabajo van en caminos convergentes, más que paralelos. Así las metodologías, con las especificaciones propias, coinciden cada vez más. No puede olvidarse que el enfoque de la gerencia es el tratamiento integral de los riesgos y a ese proceso nos encaminamos desde todos los ámbitos del riesgo.

Centrándonos en la situación, la constatación de la inexistencia de un criterio generalizado y unificado para abordar gran parte de los procesos, unido a la ausencia de herramientas de gestión, como buenas metodologías de evaluación, han conformado también la motivación a la hora de diseñar este trabajo.

En este sentido, es necesario reseñar, que los métodos propuestos, si bien se han centrado en los riesgos de seguridad y medio ambiente, son extrapolables a otros ámbitos de riesgo, en

particular a los englobados como operacionales. Serán necesarias eso sí, adaptaciones, pero la filosofía que guía estas metodologías aquí mostradas, es perfectamente aplicable a otros tipo de riesgo.

Finalmente creemos conveniente llamar la atención sobre dos cuestiones que se ponen de relieve en este trabajo.

Así nos referimos al catálogo de riesgos que se ha contemplado y sobre el que se ha construido la metodología de evaluación; se ha pretendido alcanzar a todos los riesgos por nimios que fueran, en esa pretensión, se han considerado, desde el área de seguridad, las influencias en riesgos tan escasamente tratados como el daño a la imagen o a la marca, así como el derivado de los incumplimientos legales, entre los que sobresale el relativo a LOPD. Se han tocado otras áreas de riesgo ajenas, en principio, a la seguridad y al medio ambiente; pero afectados por éstas. Una muestra evidente de la vocación integradora e integral de la Gerencia.

Por último nos referiremos a la carga conceptual que se ha plasmado en este trabajo, motivado por ese intento a que antes aludíamos de aclarar conceptos que nos lleven a la herramienta adecuada. Quizá se haya pecado de osadía o de desconocimiento científico, pero no se podía dejar pasar la constatación de las dudas que asaltan a muchos profesionales de la gerencia y de la seguridad. En esta línea se ha llegado a proponer el tratamiento del riesgo como vector, elaborando a partir de esta idea un método de evaluación, que según se ha podido probar, funciona y al menos no es ni menos bueno ni más malo que los ya consolidados. El tiempo dirá si esta línea merece ser continuada o, por el contrario se trata de una mera elucubración que no pasará de este trabajo.

BIBLIOGRAFÍA

- Andy Garlik .Estimating Risk. .. Editorial Gower. Edic. 2007.
- Aymerich Jose Ignacio, Fernández Gonzalo, García Mauricio, Iturmendi Gonzalo y Coordinación General Martínez Francisco. Gerencia de riesgos y seguros en la empresa. Editorial MAPFRE. Edic. 1998.
- Corbalán. Fernando. Sanz Gerardo. La Conquista del Azar. La Teoría de probabilidades. Edit. RBA. 2010.
- De la Calle. Miguel Angel y otros. "Riesgos ambientales. Implicaciones en la gestión empresarial". Art. Rev. Ecosostenible, nº 18-19. 2006.
- Delgado Saborit. Juana María. "La medida del riesgo ambiental. Nueva metodología para evaluar cómo afectan las actividades de la empresa al entorno natural." Art. Rev. MAPFRE SEGURIDAD, nº 107. 2007.
- Federation of European Risk Management Associations (FERMA). Estándares de Gerencia de Riesgos.
- Filgueira Otamend. Luis I. "Análisis de riesgos de contaminación accidental". Art. Internet. Aut. i. www.estrucplan.com.ar
- Fundación MAPFRE. Universidad Pontificia de Salamanca. Apuntes del XV Máster de Seguros y Gerencia de Riesgos de la Fundación MAPFRE. Universidad Pontificia de Salamanca. 2009.
- Fundación MAPFRE Estudios. Instrucciones Técnicas de Seguridad Integral. Volúmenes1 y 2 de las Instrucciones Técnicas del Concepto y Gestión de la Seguridad Integral. Abril 2004. Colección
- Fundación MAPFRE. Material didáctico del Curso de Gerencia de Riesgos y Seguros en la Empresa. Ud. Didact. 2. "Identificación y evaluación de riesgos". 2006.

- Gil. Gonzalo. Subgobernador BE. Los retos de la supervisión bancaria y las nuevas perspectivas del Acuerdo de Basilea II. Septiembre de 2003. http://www.bde.es/webbde/es/secciones/prensa/intervenpub/archivo/gonzalo_gil/sub100903.pdf (Consulta, 3 de diciembre 09)
- Gómez Déniz. Emilio. Sarabia Alegría. José María. Teoría de la Credibilidad: Desarrollo y Aplicaciones en Primas de Seguros y Riesgos Operacionales. Ed. Fundación MAPFRE. 2008
- Guía ISO / CEI 73. Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas.
- Guía ORACLE. Diagnóstico de Seguridad.
- Haider. Josef y Montero. Juan C. Arequipa. "Análisis de Riesgo de Desastres. Una herramienta importante para el manejo de microcuencas en zonas de montaña" Art..
- Ibáñez. Jesús. Basilea II: Efecto sobre el SGR, s. Banco de España. Instituciones Financieras. X Foro Iberoamericano de sistemas de garantías. Valladolid, septiembre de 2005. http://www.iberpymeonline.org/XFORO/BasileaII.pdf (Consulta, 15 octubre 09)
- ITSEMAP. "Gerencia de Riesgos. Riesgos de empresas y condiciones de aseguramiento". .Material del curso de Gerencia de Riesgos.
- Jiménez Rodriguez. Enrique José; Martín Marín. José Luis. "El nuevo acuerdo de Basilea y la gestión del riesgo operacional". Universia Bussines Review – Actualidad Económica. Tercer Trimestre 2005. http://ubr.universia.net/pdfs/UBR0032005054.pdf (Consulta, 15 de octubre 09)
- Kit Sadgrove. La gestión del riesgo en la empresa... Editorial AENOR. Edic. 2.000.
- Martínez García. Cristina. Gestion integral de riesgos corporativos como fuente de ventaja competitiva: cultura positiva del riesgo y reorganización estructural. Madrid:

FUNDACIÓN MAPFRE, Instituto de Ciencias del Seguro, Cuadernos de la Fundación. 2009.

- Nieto Gómez- Montesinos. María Ángeles. El tratamiento del riesgo operacional en Basilea II. Banco de España. Estabilidad Financiera, núm 8. 2005. http://www.bde.es/webbde/es/secciones/informes/be/estfin/numero8/estfin0807.pdf (Consulta, 18 de junio 09)
- Nieto Giménez – Montesinos. María Ángeles; Gómez Fernández. Inmaculada. Riesgo Operacional. Aspectos relevantes de los métodos de indicador básico y estándar. Cuestiones esenciales de la validación de los modelos AMA. Banco de España. R. Operacional Definición y medición. Seminario sobre Basilea II. Madrid, septiembre de 2006. http://www.bde.es/webbde/Agenda/Eventos/06/Nov/Fic/10_II_Seminario_BII_MAN-IGF_RO.pdf (Consulta, 16 de octubre 09)
- Nuria Ferré- Huget y otros. "Metales Pesados y Salud. Diseño de un software para evaluar los riesgos de exposición ambiental a través de agua, suelos y aire" Art.. Rev. MAPFRE SEGURIDAD, nº 108. 2007.
- Rao Kolluru; Steven Bartell; Robin Pitblado; Scott Stricoff. "Manual de Evaluación y Administración de Riesgos" Editorial Mc Graw Hill. 1998
- Rodríguez Trigo. Vicente. (Coordinador). Manual para el Director de Seguridad. Madrid: Editorial E.T. Estudios Técnicos, S.A. 1996.
- Sánchez Gómez-Merelo. Manual para el Director de Seguridad. Aut. Editorial E.T. Estudios Técnicos, S.A. Edic. 1996.
- Servicio de Protección Civil de Barcelona. 2002. Procedimiento de evaluación de riesgos tecnológicos en el entorno.

- Triviño Pérez. A y. Ortiz Rojas. S "Metodología para el análisis del riesgo de inundación en ramblas y ríos rambla mediterráneos" Art. De la Universidad de Alicante.
- UNESPA; Ernst & Young. SOLVENCIA II: Visión General. Septiembre 2002. http://intranet.icea.es/solvencia/Documentos/31102002_Monografico_SolvenciaII%20UNESPA.pdf. (Consulta, 21 junio 09)
- Universidad Pontificia de Comillas. ICAI-ICADE .Apuntes sobre gestión de riesgos del "Curso Superior de Dirección de Seguridad en Empresas (DSD)" de la. Curso 2008-2009.

ANEXOS

ANEXO I: Definiciones y conceptos

ANEXO II: Check list

ANEXO III: Algoritmo para establecer la relación de los riesgos con la situación identificada mediante los ítems contestados. Incluye la valoración cualitativa de los posibles riesgos. (Extracto)

ANEXO IV: Modelo para informe de análisis de riesgos (Extracto)

ANEXO V: Gráfico de Riesgos. Mapa de Riesgos

ANEXO I: Definiciones y conceptos

Activo

Conjunto de todas las capacidades, bienes, derechos, medios e intangibles, que son propiedad de una empresa, institución o individuo, o cuya posesión o derecho de explotación ostenta.

Amenaza

Causa o fuente potencial de daño a los activos tangibles e intangibles de una organización.

Análisis de Riesgos[51]

Uso sistemático de información para identificar fuentes, riesgos y vulnerabilidades, posibilitando el cálculo del riesgo.

Daño

Pérdida material o personal producida como consecuencia directa o indirecta de la materialización de una amenaza.

Evaluación de Riesgos.

Proceso que consiste en comparar el **riesgo** calculado con ciertos **criterios de riesgos** para determinar la importancia del riesgo.

La evaluación de riesgos puede utilizarse para ayudar a tomar la decisión de aceptar o tratar un riesgo.

Evaluación Cualitativa

Metodología o técnica de valoración del riesgo basada en apreciaciones de expresión no matemática que reflejan por separado o conjuntamente la probabilidad e intensidad del riesgo.

[51] Basada en la definición de la Guía ISO/CEI 73

Evaluación Cuantitativa

Metodología o técnica de valoración del riesgo basada en apreciaciones de expresión matemática que reflejan por separado o conjuntamente la probabilidad e intensidad del riesgo.

Evaluación Mixta

Metodología o técnica de valoración del riesgo que combina aspectos cualitativos con cuantificaciones mediante expresiones matemáticas, que reflejan por separado o conjuntamente la probabilidad e intensidad del riesgo.

Fuente o Factor de riesgo

Elemento o actividad que disponga de un potencial de **consecuencia.**

En el contexto de seguridad, fuente se refiere a un peligro.

En este documento es equivalente a riesgo primario.

Gerencia o Gestión de Riesgos[52]

Actividades coordinadas para dirigir y controlar una empresa en relación con el riesgo. La gestión de los riesgos incluye, por norma general, la valoración del riesgo, tratamiento del riesgo, aceptación de riesgos y comunicación de los riesgos.

Identificación de Riesgos

Proceso por el que se encuentran, enumeran y caracterizan elementos de **riesgo.**

Los elementos pueden incluir la **fuente** o peligro, **suceso, consecuencia** y **probabilidad**. La identificación de riesgos también puede reflejar las preocupaciones de los **interesados**.

Medio Ambiente

Entorno en el cual una organización opera, incluyendo el aire, el agua, la tierra, los recursos naturales, la flora, la fauna, los seres humanos y las interrelaciones entre ellos.

[52] Según definición de la Guía ISO/CEI 73

Peligro[53]

Hecho o fenómeno que puede ser causante de daños. Origen de un potencial riesgo. Sinónimo de riesgo próximo o inminente.

Riesgo[54]

Combinación de la probabilidad de un suceso y su consecuencia. Término que suele utilizarse sólo en caso de que exista, al menos, una posibilidad de consecuencia negativa.

Riesgo de Seguridad y Medio Ambiente

Del conjunto de riesgos que soportan los activos del Grupo, aquellos cuya gestión ha sido encomendada a la Organización de Seguridad y Medio Ambiente.

Seguridad

1. Condición conseguida cuando los activos están protegidos contra los riesgos.
2. Cualidad de seguro, esto es, exento de todo daño, peligro o riesgo.
3. Conjunto de medidas necesarias para alcanzar la condición anterior. En función de los activos que se protejan y de la naturaleza de las medidas, suele hablarse de diferentes tipos de seguridad, así Seguridad de la Información, Seguridad Laboral, Seguridad de las Personas, Seguridad contra Incendios, etc.

Seguridad Integral

Protección proporcionada al activo al contemplar de forma conjunta e integrada la gestión interrelacionada de todos los riesgos, o de un conjunto amplio de éstos, aun siendo de diferente naturaleza y/o respondiendo su tratamiento a diferentes disciplinas.

Tratamiento de Riesgos

Proceso de selección y puesta en aplicación de medidas para modificar el riesgo. Las medidas de tratamiento de riesgos pueden incluir evitar, optimizar, transferir o retener el riesgo.

[53] Definición según las "Instrucciones Técnicas del Concepto y Gestión de la Seguridad Integral", y según el "Diccionario MAPFRE de Seguros", ambas obras de la Fundación MAPFRE.
[54] Según definición de la Guía ISO/CEI 73

Vulnerabilidad[55]

1. Referente a la condición de una persona, sistema o elemento que indica la posibilidad de que resulten dañadas ante un riesgo determinado.

2. Debilidad de un sistema, elemento o instalación, que posibilita o incrementa la probabilidad de materialización de una amenaza, o el posible daño por ésta producido

Riesgo

Combinación de la probabilidad de un suceso y su consecuencia. Término que suele utilizarse sólo en caso de que exista, al menos, una posibilidad de consecuencia negativa.

Riesgo Agregado o Riesgo Tipo

Riesgo total referido a un tipo de los del catálogo que soporta el activo analizado. Es función de los riesgos primarios o factores de riesgo de ese tipo que se hayan identificado.

Así se puede hablar de Riesgo Tipo o Agregado de Intrusión, o simplemente Riesgo de Intrusión, para un edificio.

Vulnerabilidad

1. Referente a la condición de una persona, sistema o elemento que indica la posibilidad de que resulten dañadas ante un riesgo determinado.

2. Debilidad de un sistema, elemento o instalación, que posibilita o incrementa la manifestación de un riesgo.

[55] Definición según las "Instrucciones Técnicas del Concepto y Gestión de la Seguridad Integral", de la Fundación MAPFRE y adoptado en el ámbito de la Seguridad de la Información.

ANEXO II: Check list para identificar Riesgos de Seguridad y Medio ambiente.

1. DATOS GENERALES

País	
Ciudad Provincia Municipio	
Nombre del Edificio:	
Dirección:	
SST/JSCM/JS	

Fecha Inspección:	

.

Número de Plantas		
Plantas:		Incluyendo Planta Baja
Sótanos:		Incluyendo semisótanos

Nombres Equipo Evaluador	
1.	
2.	
3.	

2. CARACTERÍSTICAS DEL EDIFICIO:

Tipo de edificio

2.1	¿Es un complejo de varios edificios ?	N/A
2.2	¿Se puede acceder al edificio directamente desde la vía?	N/A
2.3	¿Está el edificio aislado?	N/A
2.4	¿El edificio tiene parcela?	N/A
2.5	¿El edificio tiene valla?	N/A
2.6	Si dispone de alguna de las particularidades anteriormente descritas ¿Se tienen en cuenta en la gestión de la seguridad?	N/A

Actividades

2.7	Si el edificio contiene un museo, ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A
2.8	Si el edificio contiene aulas de formación, ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A
2.9	Si es un centro del automóvil (PPR), ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A
2.10	Si está la instalación localizada en un centro comercial, ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A
2.11	Si es un centro médico, ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A
2.12	Si es una oficina directa, ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A
2.13	Si hay oficina bancaria en el edificio, ¿Están controlados los posibles riesgos asociados a esta actividad?	N/A

3. RIESGOS GLOBALES: Seleccione las características que pueda tener la instalación

Posibles riesgos por proximidad a:

3.1	Si el edificio está localizado próximo a un Río / Lago / Embalse ¿están controlados los posibles riesgos asociados a este hecho?	N/A
3.2	Si el edificio está localizado próximo a la costa ¿están controlados los posibles riesgos asociados a este hecho?	N/A
3.3	Si el edificio está localizado próximo a una autopista ¿están controlados los posibles riesgos asociados a este hecho?	N/A
3.4	Si hay líneas de alta tensión proximas a la edificación ¿están controlados los posibles riesgos asociados a este hecho?	N/A
3.5	Si hay gaseoducto o gasolinera próximos a la edificación ¿están controlados los posibles riesgos asociados a este hecho?	N/A

Zona Geográfica

3.6	Si el edificio está localizado en zona de riesgo sísmico ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.7	Si el edificio está localizado en zona que presenta tormentas eléctricas ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.8	Si el edificio está localizado en zona de riesgo de huracanes ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.9	Si el edificio está localizado en zona donde se presentan nevadas ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.10	Si el edificio está localizado en zona donde se presentan heladas ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.11	Si el edificio está localizado en zona de riesgo de avalancha o aludes ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.12	Si el edificio está localizado en zona con actividad volcánica ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.13	Si el edificio está localizado en zona con altas precipitaciones ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A
3.14	Si el edificio está localizado en zona donde se presentan vientos fuertes ¿Cuenta con la protección y medios de seguridad exigidos legal y/o técnicamente?	N/A

Otros

3.15	Si el edificio está localizado en zona con amenaza o vulnerabilidad terrorista, o una persona del edificio se encuentra bajo esta amenza: ¿Cuenta con la protección y medios de seguridad para controlar el riesgo?	N/A
3.16	Si hay empresas o actividades próximas que puedan generar daños a la instalación o a sus ocupantes ¿Cuenta con la protección y medios de seguridad para controla	N/A
3.17	Si el entorno es social o delincuencialmente conflictivo, ¿Cuenta con la protección y medios de seguridad para controlar el riesgo?	N/A
3.18	¿Cuenta la instalación con Pararrayos?	N/A
3.19	¿Está la central de bomberos a menos de 5 km ó de 5 min? (Indique cuál es la distancia a la central de Bom	Seleccionar... N/A

Planes del Edificio/ Planes de Seguridad		Fecha de Actualización	
3.20	¿Aplica un plan de seguridad específico para la edificación?		N/A
3.21	¿Cuenta con certificación medioambiental?		N/A
3.22	¿Tiene implementado un plan de autoprotección?		N/A
3.23	¿Se aplican las medidas de seguridad de la información establecidas por la empresa?		N/A
3.24	¿Conoce el manual de gestión de crisis del plan de continuidad de negocio?		N/A
3.25	¿Tiene el edificio licencia de actividad?		N/A
3.26	¿Existe alguna normativa local específica, regional, nacional o por la actividad desarrollada en el edificio, en cualquiera de los ámbitos: protección de datos, incendio, planes de emergencia, seguridad privada, entre otras?		N/A
3.27	¿Se aplica la normativa especifica reseñada en el número anterior?		N/A

Observaciones:

4. ZONAS EDIFICIO

4.1 VALLADO (VALLA/ CERCA) (PERIMETRAL Y COMPLETA)

APLICA: NO

4.1.1	¿Ofrece la valla resistencia adecuada a la intrusión?	N/A
4.1.2	¿Cuenta con murete para evitar el acceso por fuerza de vehículos?	N/A
4.1.3	¿El estado de mantenimiento de la valla es bueno?	N/A
4.1.4	¿Está securizada la valla para detectar intentos de vulnerarla?	N/A
4.1.5	¿Dificulta la valla la escalada?	N/A
4.1.6	¿Está vigilada la valla?	N/A
4.1.7	¿En la zona existe circuito cerrado de televisión?	N/A
4.1.8	¿Tiene la valla iluminación suficiente?	N/A
4.1.9	¿Cuenta la valla con iluminación sorpresiva?	N/A
4.1.10	¿Se cierran las puertas de acceso del vallado fuera del horario laboral?	N/A
4.1.11	¿Tienen las puertas del vallado resistencia suficiente para dificultar su vulneración?	N/A
4.1.12	¿Está controlado el acceso por todas las puertas?	N/A
4.1.13	¿Permanecen cerradas las puertas secundarias habitualmente?	N/A
4.1.14	¿Tienen habilitados las puertas accesos para peatones?	N/A
4.1.15	¿Cuentan con barreras o medios para el control de vehículos los accesos principal y de uso habitual?	N/A
4.1.16	¿Cuentan con tornos o medios para el control de peatones los accesos principales y uso habitual?	N/A
4.1.17	¿Se dispone de interfono?	N/A

Observaciones:

4.2 CENTRO DE CONTROL (CC) Y/O SALA DE SEGURIDAD (SS) (NO APLICAR A

APLICA: NO

4.2.1	¿Está vigilada la zona de acceso al centro de control?	N/A
4.2.2	¿En la zona existe circuito cerrado de televisión?	N/A
4.2.3	¿Se controla el acceso al interior del Centro de Control (CC/SS), permitiéndoselo solo a personal autorizado?	N/A
4.2.4	¿Son resistentes y seguras la estructura y puertas, dificultando o impidiendo la intrusión?	N/A
4.2.5	¿Se cierra con llave el CC/SS, si no está activado permanentemente, y se controla la misma?	N/A
4.2.6	¿Cuenta el CC/SS con detector de apertura o volumétrico, si no está activado permanentemente?	N/A
4.2.7	¿Cuenta con protección contra incendios?	N/A
4.2.8	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores de 2 mts?	N/A
4.2.9	¿Se detecta la presencia de objetos, equipos o elementos que puedan provocar la ignición?	N/A
4.2.10	¿Se aprecian líquidos o productos inflamables sin control?	N/A
4.2.11	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.2.12	¿Se aprecian residuos incontrolados?	N/A
4.2.13	¿Se aprecia desorden y/o suciedad?	N/A
4.2.14	¿Se aplica un protocolo de actuación para controlar el acceso de vehículos a la instalación?	N/A
4.2.15	¿Se aplica un protocolo de actuación para controlar el acceso de peatones a la instalación?	N/A
4.2.16	¿Se entrega tarjeta de acreditación a los vehículos y peatones que acceden a la instalación?	N/A
4.2.17	¿Se aplica un protocolo para la recepción y distribución de paquetería y correspondencia?	N/A
4.2.18	¿Se aplica un protocolo de acceso para proveedores?	N/A
4.2.19	¿Se dispone de copia del plan de autoprotección y es comunicado de los bomberos?	N/A
4.2.20	¿Están involucrados en el plan de emergencia los vigilantes y personal del centro del control, y conocen su rol?	N/A
4.2.21	¿Hay advertencias escritas sobre la captación de datos personales y están adecuadas a la normativa vigente?	N/A

Observaciones:

4.3 PARCELA

APLICA | NO

4.3.1	¿Se aplica un protocolo para coordinar la seguridad, Si la parcela no es de MAPFRE?	N/A
4.3.2	¿Está vigilada la parcela?	N/A
4.3.3	¿Facilita la parcela el ocultamiento?	N/A
4.3.4	¿Hay elementos que faciliten el acceso al edificio (Árboles, objetos, etc.) en la parcela?	N/A
4.3.5	¿Se controlan los vehículos que permanecen en la parcela?	N/A
4.3.6	¿Se prohíbe que pernocten vehículos en la parcela?	N/A
4.3.7	¿Está señalizada la zona de estacionamiento exterior?	N/A
4.3.8	¿Está controlado el acceso de peatones al parking?	N/A
4.3.9	¿Se encuentran señalizados los accesos al o desde el parking?	N/A
4.3.10	¿Se dispone de algún control adicional en el acceso de vehículos desde la parcela al parking? (Especificar)	N/A
4.3.11	¿Existen objetos, equipos, materiales o productos que supongan un aumento de la carga de fuego?	N/A
4.3.12	¿Cuenta con medios de protección contra incendios?	N/A
4.3.13	¿Cuenta la parcela con BIES y/o Hidrantes?	N/A
4.3.14	¿Facilita la parcela el acceso de bomberos al edificio?	N/A
4.3.15	¿Está la parcela cuidada y mantenida?	N/A
4.3.16	¿Hay en la parcela relieves u objetos que puedan causar un accidente?	N/A
4.3.17	Si existen objeto de valor en la parcela (Ejemplo: Esculturas y Obras de arte) ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.3.18	¿Se deposita algún tipo de residuo en la parcela de forma desontrolada?	N/A
4.3.19	En la parcela se aprecia algún tipo de contaminante o producto peligroso	N/A
4.3.20	¿Existe entre la vegetación de la parcela alguna especie protegida?	N/A

Observaciones:

4.4 FACHADA Y ESTRUCTURA, PERIMETRO INTERIOR

APLICA | NO

4.4.1	¿Se vigila el perímetro interior por algún medio?	N/A
4.4.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.4.3	¿Facilita la fachada la intrusión al edificio?	N/A
4.4.4	¿Facilitan las ventanas la intrusión al edificio?	N/A
4.4.5	¿Se detecta la apertura de las ventanas de la planta baja y primeras accesibles?	N/A
4.4.6	¿Se cierra la puerta principal tras finalizar la jornada laboral?	N/A
4.4.7	¿Se cuenta con detectores de apertura de puertas exteriores?	N/A
4.4.8	¿Se puede acceder al edificio desde los edificios próximos?	N/A
4.4.9	¿Son blindadas o de resistencia adecuada las ventanas, cristalerías de la planta baja y las plantas accesibles mediante escalamiento, para evitar su rotura mediante el lanzamiento de un objeto contundente?	N/A
4.4.10	¿Permanecen habitualmente cerradas las puertas secundarias, permitiendo solo el paso a personas autorizadas?	N/A
4.4.11	¿Existen objetos o elementos en la fachada que pueden provocar daños? (Especificar)	N/A
4.4.12	¿Se mantiene adecuadamente la fachada?	N/A

Observaciones:

4.5 TRANSFORMADOR Y SUMINISTROS DE ENERGIA

APLICA | NO

4.5.1	¿Está bajo la responsabilidad MAPFRE el recinto del transformador?	N/A
4.5.2	¿Se han adoptado medidas de coordinación con la compañía eléctrica responsable?	N/A
4.5.3	Si el transformador se encuentra dentro del edificio, ¿esto está contemplado en el plan de outoprotección?	N/A
4.5.4	¿Está cerrado con llave habitualmente el recinto del transformador?	N/A
4.5.5	¿Se dispone de un protocolo de actuación para hacer frente a cualquier eventualidad procedente del transformador, y el mismo está contemplado en el plan de autoprot	N/A
4.5.6	¿Se controla el acceso al transformador? (solo se permite a personal autorizado)	N/A
4.5.7	¿Tiene acceso al transformador el personal autorizado de MAPFRE, para hacer frente a una emergencia?	N/A
4.5.8	¿Está ventilado el transformador?	N/A
4.5.9	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.5.10	¿Cuenta el transformador con protección contra incendios?	N/A
4.5.11	¿Se aprecian sustancias contaminantes o peligrosas cercanas al transformador?	N/A
4.5.12	¿Existe algún protocolo para reaccionar ante un incidente ocasionado por las tomas externas de suministro de energía?	N/A

Observaciones:

4.6 OFICINA DIRECTA / OFICINA COMERCIAL

APLICA: NO

4.6.1	¿Está vigilado el acceso exterior a la oficina directa?	N/A
4.6.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.6.3	¿Dificultan la intrusión a la Oficina Directa, la estructura y puertas?	N/A
4.6.4	¿Se controla el cierre y apertura de puertas (interior y exterior)?	N/A
4.6.5	¿Tienen resistencia los vidrios exteriores para evitar su rotura ante el lanzamiento de objetos?	N/A
4.6.6	¿Se cuenta con detección de apertura de puertas exteriores?	N/A
4.6.7	¿Cuenta el recinto con detectores de movimiento?	N/A
4.6.8	¿Se controlan los accesos hacia el interior del edificio?	N/A
4.6.9	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.6.10	¿Cuenta con extintores adecuados?	N/A
4.6.11	¿Cuenta con detección automática de incendios?	N/A
4.6.12	¿Cuenta con BIES próxima?	N/A
4.6.13	¿Existen conducciones de agua que pueden dañar la documentación? (Conducciones en mal estado o que por sus características sea probable su rotura)	N/A
4.6.14	¿Se aprecia suciedad y desorden?	N/A
4.6.15	¿Están los contenedores fuera del alcance de ajenos?	N/A
4.6.16	¿Se arrojan a la papelera documentos sensibles para MAPFRE o que contengan datos personales?	N/A
4.6.17	¿Hay libre acceso a documentos sensibles para MAPFRE o que contengan datos personales?	N/A
4.6.18	¿Hay documentos sensibles para MAPFRE o con datos personales en las mesas de trabajo, papeleras y estanterías abiertas, posibilitando el acceso por terceros?	N/A
4.6.19	¿Se encuentran las zonas ofimáticas en lugares controlados por la vista de los empleados o fuera del paso?	N/A
4.6.20	¿Hay destructoras o contenedores de documentos?	N/A
4.6.21	¿Se aprecian residuos incontrolados?	N/A
4.6.22	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.6.23	Si existen objeto de valor en la oficina directa ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.6.24	¿Es correcta y adecuada la señalización e iluminación de emergencia?	N/A
4.6.25	¿Está prohibido fumar?	N/A

Observaciones:

4.7 PARKING

APLICA: NO

4.7.1	¿Es el parking de uso exclusivo para la empresa?	N/A
4.7.2	¿Es el parking de uso exclusivo para los usuarios del edificio?	N/A
4.7.3	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.7.4	¿Se utiliza el parking para otros fines que implique el acceso regular de ajenos (por ejemplo PPR)?	N/A
4.7.5	¿Está vigilado el parking?	N/A
4.7.6	¿Se controla el acceso de vehículos al parking?	N/A
4.7.7	¿Se controla el acceso de peatones al parking?	N/A
4.7.8	¿Se verifica que los vehículos estacionados en el parking están autorizados para ocupar esa plaza?	N/A
4.7.9	¿Permanece el parking cerrado fuera del horario laboral?	N/A
4.7.10	¿Se realiza control de vehículos que permanecen en el parking fuera del horario laboral?	N/A
4.7.11	¿Son resistentes las puertas del parking?	N/A
4.7.12	¿Existe detección de apertura de las puertas del parking?	N/A
4.7.13	¿Existen huecos o zonas desprotegidas en la estructura que faciliten la intrusión?	N/A
4.7.14	¿Se controla el acceso desde el parking al interior del edificio?	N/A
4.7.15	¿Impiden las salidas de emergencia al exterior el paso libre hacia el interior del parking?	N/A
4.7.16	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 mts?	N/A
4.7.17	¿Hay elementos o equipos susceptibles de provocar un incendio?	N/A
4.7.18	¿Existe detección automática de incendios en el parking?	N/A
4.7.19	¿Cuenta el parking con extintores adecuados?	N/A
4.7.20	¿Existen bocas para incendios equipadas en el parking?	N/A
4.7.21	¿Cuenta el parking con extinción automática de incendios?	N/A
4.7.22	¿Está el parking sectorizado contra incendios?	N/A
4.7.23	¿Cuenta el parking con las salidas de emergencia requeridas legalmente?	N/A
4.7.24	¿Cuenta el parking con la señalización de incendios y circulación?	N/A
4.7.25	¿Cuenta el parking cuenta con iluminación de emergencia en perfecto estado de funcionamiento?	N/A
4.7.26	¿Existen conducciones o depósitos de agua, que puedan causar una inundación? (elementos en mal estado o que por sus características sea posible su rotura)	N/A
4.7.27	¿Se aprecian residuos incontrolados?	N/A
4.7.28	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.7.29	Si existen objeto de valor en el parking (Ejemplo: Esculturas y Obras de Arte) ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.7.30	¿Son las normas de circulación interior óptimas para controlar el tráfico interno y evitar o reducir accidentes?	N/A
4.7.31	¿Existen equipos o elementos que incrementen de forma notable el nivel sonoro?	N/A
4.7.32	¿Es suficiente la ventilación que se aprecia?	N/A
4.7.33	¿Se aprecia suciedad y desorden?	N/A
4.7.34	¿Se controla de algún modo la salida de vehículos del parking?	N/A

Observaciones:

4.8 CENTRO DEL AUTOMOVIL - PPR / CENTRO DE PERITAJE

APLICA | NO

4.8.1	¿Se encuentra vigilado el PPR?	N/A
4.8.2	¿Se controlan los vehículos que acceden al PPR?	N/A
4.8.3	¿Se controlan los vehículos que permanecen en el PPR?	N/A
4.8.4	¿Está cerrado con llave fuera de horario laboral?	N/A
4.8.5	¿Son resistentes las paredes y puertas del PPR?	N/A
4.8.6	¿Existe detección de apertura de las puertas del PPR?	N/A
4.8.7	¿Se accede libremente al interior de las oficinas desde el PPR?	N/A
4.8.8	¿Existe detección de movimiento en la oficina del PPR?	N/A
4.8.9	¿Existen objetos o equipos que supongan un incremento en la carga, o apilaciones mayores a 2 mts?	N/A
4.8.10	¿Cuenta el PPR con extintores adecuados?	N/A
4.8.11	¿Existe detección automática de incendios?	N/A
4.8.12	¿Esta señalizada la zona de estacionamiento?	N/A
4.8.13	¿Existen bocas incendios equipadas en el PPR?	N/A
4.8.14	¿Cuenta el PPR con salidas de emergencia? (Por lo menos las requeridas legalmente)	N/A
4.8.15	¿Se aprecian residuos incontrolados?	N/A
4.8.16	¿Cuenta con contenedor para reciclaje de papel?	N/A
4.8.17	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.8.18	¿Pueden acceder fácilmente a la documentación de trabajo personas ajenas a la dependencia? (por ejemplo: Encima de mesas)	N/A
4.8.19	¿Se guarda bajo llave la documentación sensible, clasificada o con datos personales?	N/A
4.8.20	Si existen objeto de valor en el PPR ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A

Observaciones:

4.9 CUARTOS TECNICOS (Cuarto de Maquinas, Zona Humca, UPS / Generador)

APLICA | NO

4.9.1	¿Se vigila de algún modo el acceso a los cuartos técnicos?	N/A
4.9.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.9.3	¿Se controla el acceso permitiéndoselo únicamente a autorizados?	N/A
4.9.4	¿Están cerrados con llave habitualmente?	N/A
4.9.5	¿Se controla el acceso a los cuartos técnicos con tarjeta?	N/A
4.9.6	¿Son seguras las puertas y estructuras, dificultando o impidiendo la intrusión?	N/A
4.9.7	¿Existen detectores de movimiento o detectores de intrusión por ventanas, puertas, etc.?	N/A
4.9.8	¿Existen conducciones o depósitos de agua susceptibles a provocar una inundación?	N/A
4.9.9	¿Se detectan incrementos de temperatura y humedad?	N/A
4.9.10	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.9.11	¿Se aprecian líquidos o productos inflamables descontrolados que puedan aumentar la carga de fuego por encima de lo habitual?	N/A
4.9.12	¿Cuenta con detección automática?	N/A
4.9.13	¿Cuenta con BIES próximas?	N/A
4.9.14	¿Están diseñados y proporcionados los equipos contra incendios a la carga de incendio existente?	N/A
4.9.15	¿Existe detección de gas en la sala de calderas?	N/A
4.9.16	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.9.17	¿Se aprecian residuos incontrolados?	N/A
4.9.18	¿Se gestionan las baterías en desuso (UPS) conforme al protocolo de medio ambiente?	N/A
4.9.20	¿Disponen los cuartos de ventilación adecuada?	N/A
4.9.21	¿Se aprecia desorden y/o suciedad?	N/A
4.9.22	¿Se realizan los mantenimientos adecuados de la maquinaria y equipos de la instalación?	N/A
4.9.23	Si existen objeto de valor en los cuartos técnicos ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.9.24	¿Se encuentra el aljibe en el sótano?	N/A

Observaciones:

4.10 ZONA RESIDUOS

APLICA | NO

4.10.1	¿Está identificada la zona de residuos?	N/A
4.10.2	¿Está separada físicamente la zona de residuos del resto de zonas?	N/A
4.10.3	¿Se encuentra pavimentada y bajo cubierta la zona de residuos?	N/A
4.10.4	¿Están separados e identificados los residuos de acuerdo a su naturaleza y peligrosidad?	N/A
4.10.5	¿Se encuentran en esta zona documentos o papeles con datos personales o sensibles para MAPFRE?	N/A
4.10.6	¿Existe y se aplica un protocolo medioambiental para gestionar los residuos?	N/A
4.10.7	¿Se aprecia desorden y/o suciedad?	N/A
4.10.8	¿Existen conducciones o depósitos de agua que puedan generar un daño ambiental?	N/A
4.10.9	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.10.10	¿Se cuenta con protección contra incendios adecuada con la naturaleza y carga de fuego de los residuos?	N/A
4.10.11	¿Se controla el acceso a la zona de residuos, permitiéndolo solo al personal autorizado?	N/A
4.10.12	¿Está prohibido fumar?	N/A

Observaciones:

4.11 DEPOSITO DE COMBUSTIBLE (APLICA CUALQUIER DEPOSITO DE ALMACENAJE)(BODEGAS -DEPÓSITOS)

APLICA | NO

4.11.1	¿Está vigilada la zona de combustibles?	N/A
4.11.2	¿Están los depósitos en un recinto cerrado con llave?	N/A
4.11.3	¿Se controlan las llaves?	N/A
4.11.4	¿Puede acceder al depósito solo personal autorizado?	N/A
4.11.5	¿Existen equipos o elementos en las proximidades que puedan generar la ignición?	N/A
4.11.6	¿Cuenta con detección automática de incendios?	N/A
4.11.7	¿Cuenta con extintores apropiados?	N/A
4.11.8	¿Cuenta el depósito con BIES?	N/A
4.11.9	¿Se aprecia desorden o suciedad?	N/A
4.11.10	¿Se aprecian residuos incontrolados en esta zona?	N/A
4.11.11	¿Hay sustancias contaminantes o peligrosas sin control?	N/A
4.11.12	¿Cuenta con dispositivos anti derrame?	N/A
4.11.13	¿Se realizan inspecciones periódicas para detectar o prevenir distintas fugas o vertidos?	N/A
4.11.14	¿Se aplica algún protocolo de actuación ante vertidos?	N/A
4.11.15	¿Se dispone de sustancias para actuar ante vertidos?	N/A
4.11.16	¿Cuenta con detector de fugas?	N/A
4.11.17	¿Es estanco o cuenta con cubeto?	N/A
4.11.18	¿Está prohibido fumar?	N/A

Observaciones:

4.12 ALMACENES, CUARTOS DE MANTENIMIENTO Y LIMPIEZA (BODEGAS -DEPÓSITOS)

APLICA | NO

4.12.1	¿Está vigilada la zona?	N/A
4.12.2	¿Está cerrado con llave habitualmente?	N/A
4.12.3	¿Se controlan las llaves?	N/A
4.12.4	¿Solo puede acceder a los cuartos personal autorizado?	N/A
4.12.5	Si existen objeto de valor en el almacén (Ejemplo: Esculturas y Obras de Arte) ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.12.6	¿Se aprecian sustancias contaminantes o peligrosas sin control?	N/A
4.12.7	¿Existen objetos o equipos que supongan un incremento en la carga de fuego, o apilaciones mayores de 2 m?	N/A
4.12.8	¿Cuenta con detección automática de incendios?	N/A
4.12.9	¿Dispone de extintores adecuados?	N/A
4.12.10	¿Se aprecian residuos incontrolados en esta zona?	N/A
4.12.11	¿Está prohibido fumar?	N/A

Observaciones:

4.13 FOSA SÉPTICA/DEPURADORA

APLICA NO

4.13.1	¿Existe riesgo de inundación?	N/A
4.13.2	¿Se vacía periódicamente la fosa séptica o depuradora?	N/A
4.13.3	¿Se realiza el vaciado o vertido de la fosa o depuradora de acuerdo con el protocolo establecido por Medio Ambiente?	N/A
4.13.4	¿Se revisa que no hay filtraciones de forma periódica?	N/A
4.13.5	¿Están controlados los posibles olores? (no existe presencia de malos olores por la fosa séptica / depuradora)	N/A
4.13.6	¿Es posible que una persona caiga en la fosa o depuradora?	N/A
4.13.7	¿Se trata y se mantiene de acuerdo con la legislación aplicable y protocolos de medio ambiente?	N/A

Observaciones:

4.14 ARCHIVOS, SALA DE COMUNICACIONES Y /O CPD

APLICA NO

4.14.1	¿Están vigilados los archivos?	N/A
4.14.2	¿Se capta el acceso al recinto mediante circuito cerrado de televisión?	N/A
4.14.3	¿Está cerrado habitualmente e impide el libre acceso?	N/A
4.14.4	¿Cuenta con detección de movimiento?	N/A
4.14.5	¿Se controla el acceso, permitiéndoselo únicamente a los autorizados?	N/A
4.14.6	¿Se hace el control de accesos mediante tarjeta?	N/A
4.14.7	¿Es segura la estructura, dificulta o impide la intrusión?	N/A
4.14.8	¿Se cuenta con detección de apertura de puertas?	N/A
4.14.9	¿Comparte el uso con otras funciones?	N/A
4.14.10	¿Existen objetos o equipos que supongan un incremento en la carga de fuego, o apilaciones mayores de 2 m?	N/A
4.14.11	¿Se detecta la presencia de productos inflamables sin control?	N/A
4.14.12	¿Cuenta con extintores adecuados?	N/A
4.14.13	¿Cuenta con detección automática de incendios?	N/A
4.14.14	¿Cuenta con extinción automática de incendios adecuada a la naturaleza del continente?	N/A
4.14.15	¿Cuenta con BIES próximas?	N/A
4.14.16	¿Se detecta la presencia de productos, equipos o elementos que puedan provocar la ignición?	N/A
4.14.17	¿Se aprecia suciedad y desorden?	N/A
4.14.18	¿Existen conducciones o depósitos de agua que puedan provocar una inundación o daños a la documentación? (elementos en mal estado o que por sus características sea posible su rotura)	N/A
4.14.19	¿Se aprecia humedad?	N/A
4.14.20	¿Hay detector de humedad y temperatura?	N/A
4.14.21	¿Se aprecian residuos incontrolados?	N/A
4.14.22	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.14.23	¿Está prohibido fumar?	N/A
4.14.24	¿Se aplica algún criterio para archivo de la documentación?	N/A
4.14.25	Si se comparte el archivo entre varias entidades, ¿existen y se aplican protocolos de uso?	N/A
4.14.26	¿Está designado responsable del archivo?	N/A
4.14.27	¿En los archivos, salas de comunicaciones, CPD se controla la aparición de plagas, roedores, insectos, etc.?	N/A

Observaciones:

4.15 HALL (LOBBYS)

APLICA NO

4.15.1	¿Está vigilado?	N/A
4.15.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.15.3	¿Está vigilado el hall de la planta baja (PB) por medios humanos?	N/A
4.15.4	¿Existe detección de movimiento?	N/A
4.15.5	¿Se controla el personal que accede al edificio en PB?	N/A
4.15.6	¿Se utilizan medios electrónicos o mecánicos para controlar el acceso al edificio, como torno, barrera, etc.?	N/A
4.15.7	¿Existen objetos o equipos que supongan un incremento en la carga de fuego, o apilaciones mayores de 2 mts?	N/A
4.15.8	¿Están señalizadas las salidas?	N/A
4.15.9	¿Dispone de planos "Está usted aquí"?	N/A
4.15.10	¿Se cuenta con iluminación de emergencia en perfecto estado de funcionamiento?	N/A
4.15.11	¿Existe protección contra incendios adecuada?	N/A
4.15.12	¿Existen en esta zona objetos de valor? (Ejemplo: Esculturas y Obras de arte) (en caso de que existan menciónense en observaciones)	N/A
4.15.13	¿Se informa, con los requerimientos de la LOPD, sobre la captación de imágenes?	N/A
4.15.14	¿Se aprecia desorden y suciedad?	N/A

Observaciones:

4.16 ASCENSORES Y ESCALERAS

APLICA | NO

4.16.1	¿Se accede libremente a los mismos desde cualquier planta permitiendo el acceso al interior de las zonas?	N/A
4.16.2	¿Se controla el acceso al ascensor de proveedores, o el mismo no existe?	N/A
4.16.3	¿Disponen las escaleras de iluminación y señalización de emergencias?	N/A

Observaciones:

4.17 SALIDAS DE EMERGENCIA

APLICA | NO

4.17.1	¿Hay salida de emergencia en todas las plantas?	N/A
4.17.2	¿Disponen las salidas de iluminación y señalización de emergencia?	N/A
4.17.3	¿Permiten las salidas de emergencia, la entrada libre?	N/A
4.17.4	¿Están habitualmente cerradas las salidas de emergencia?	N/A
4.17.5	¿Tienen detector de apertura las salidas de emergencia?	N/A
4.17.6	¿Se vigila el acceso a las salidas de emergencia?	N/A
4.17.7	¿Tienen las salidas de emergencia aviso de "Solo abrirse en caso de Emergencia"?	N/A
4.17.8	¿Están expeditas las salidas de emergencia?	N/A
4.17.9	¿Son resistentes al fuego (RF) las puertas de emergencia?	N/A

Observaciones:

4.18 COCINA, CAFETERÍA

APLICA | NO

4.18.1	¿Están vigilados la cocina o el acceso?	N/A
4.18.2	¿En la zona existe circuito cerrado de televisión?	N/A
4.18.3	¿Están cerradas con llave fuera del horario laboral?	N/A
4.18.4	¿Se cierran con llave las dependencias y armarios interiores?	N/A
4.18.5	¿Se controlan las llaves?	N/A
4.18.6	¿Se controla el acceso fuera del horario de apertura, permitiéndoselo sólo a los autorizados?	N/A
4.18.7	¿Cuenta el recinto con detectores de movimiento?	N/A
4.18.8	¿Se detectan las fugas de contaminantes o gases tóxicos de las cámaras frigoríficas?	N/A
4.18.9	¿Disponen las cámaras frigoríficas de algún sistema para impedir que alguien quede encerrado?	N/A
4.18.10	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.18.11	¿Se detecta la presencia de productos inflamables sin control?	N/A
4.18.12	¿Se detectan objetos, equipos o elementos que puedan provocar una ignición?	N/A
4.18.13	¿Cuenta con extintores adecuados?	N/A
4.18.14	¿Cuenta con detección automática de incendios?	N/A
4.18.15	¿Cuentan la cocina y cafetería con extinción automática de incendios?	N/A
4.18.16	¿Cuenta con BIES próximas?	N/A
4.18.17	¿Se cuenta con detección de apertura de puertas?	N/A
4.18.18	¿Cuenta con detectores de gas?	N/A
4.18.19	¿Existen conducciones ó depósitos de agua que pueden provocar una inundación? (Elementos que no sean propios de la instalación, en mal estado o que por sus características sea posible su rotura)	N/A
4.18.20	¿Se aprecian residuos incontrolados?	N/A
4.18.21	¿Se gestionan los residuos adecuadamente?	N/A
4.18.22	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.18.23	¿Se aprecia suciedad y desorden?	N/A
4.18.24	Si existen objeto de valor ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.18.25	¿Se realiza algún tipo de control de alimentos por el servicio de sanidad?	N/A
4.18.26	¿Se realizan los mantenimientos adecuados?	N/A
4.18.27	¿Está prohibido fumar?	N/A

Observaciones:

4.19 CLÍNICA,CONSULTORIO y/ o DESPACHO MÉDICO

APLICA: NO

4.19.1	¿Está vigilada la zona?	N/A
4.19.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.19.3	¿Permanecen cerradas con llave cuando no están ocupadas?	N/A
4.19.4	¿Se controla el acceso permitiéndolo solo a los autorizados?	N/A
4.19.5	¿Se controla el acceso fuera del horario de atención a pacientes por medio de tarjeta?	N/A
4.19.6	¿Dificultan la intrusión la estructura y puertas?	N/A
4.19.7	¿Se detecta la apertura de las puertas de acceso a la clínica?	N/A
4.19.8	¿Cuenta el recinto con detectores de movimiento?	N/A
4.19.9	¿Son accesibles los archivos de historiales y/o radiografías solamente para personal expresamente autorizado?	N/A
4.19.10	¿Se guardan bajo llave los documentos que contienen datos personales?	N/A
4.19.11	¿Impide la estructura de los despachos que las conversaciones se escuchen fuera de los mismos?	N/A
4.19.12	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.19.13	¿Se detecta la presencia de productos inflamables sin control?	N/A
4.19.14	¿Se detectan objetos, equipos o elementos que puedan provocar una ignición?	N/A
4.19.15	¿Cuenta con extintores adecuados?	N/A
4.19.16	¿Cuenta con detección automática de incendios?	N/A
4.19.17	¿Cuenta con BIES próximas?	N/A
4.19.18	¿Existen conducciones o depósitos de agua que puedan dañar documentos o equipos? (elementos en mal estado o que por sus características sea posible su rotura)	N/A
4.19.19	¿Cuenta con señalización e iluminación de emergencia?	N/A
4.19.20	¿Se aprecian residuos incontrolados?	N/A
4.19.21	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.19.22	¿Se gestionan los residuos adecuadamente?	N/A
4.19.23	¿Se aprecia suciedad y desorden?	N/A
4.19.24	¿Se encuentra el recinto en buen estado de mantenimiento?	N/A
4.19.25	Si existen objetos de valor ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.19.26	¿Dispone de equipos de radiología, rayos "X", medicina nuclear, etc..?	N/A
4.19.27	¿Está prohibido fumar?	N/A

Observaciones:

4.20 CORREOS (Zona de sacas y valijas, casilleros de comunicaciones)

APLICA: NO

4.20.1	¿Está vigilada la zona de correos?	N/A
4.20.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.20.3	¿Se encuentra cerrado con llave el recinto o zona cuando no está ocupado?	N/A
4.20.4	¿Cuenta el recinto o zona con detección de apertura de puertas?	N/A
4.20.5	¿Existe en la zona o recinto detección de movimientos?	N/A
4.20.6	¿Pueden acceder a los casilleros asignados para correspondencia solamente los autorizados?	N/A
4.20.7	¿Están implementados protocolos de actuación ante la detección de un paquete o carta sospechosos?	N/A
4.20.8	¿Se aplica un protocolo de entrega de paquetería que permita documentar dicha entrega?	N/A
4.20.9	¿Se encuentran en un lugar seguro y controlado en todo momento valija y paquetería, en especial durante la fase de recogida y salida de correos?	N/A
4.20.10	¿Se aprecia humedad?	N/A
4.20.11	¿Son fácilmente accesibles las valijas, correspondencia y/o casilleros de correos para ajenos al servicio?	N/A
4.20.12	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.20.13	¿Se detecta la presencia de productos inflamables sin control?	N/A
4.20.14	¿Cuenta con extintores adecuados?	N/A
4.20.15	¿Cuenta con BIES próximas?	N/A
4.20.16	¿Existen conducciones o depósitos de agua que puedan provocar daños a la documentación? (Elementos en mal estado o que por sus características sea posible su r	N/A
4.20.17	¿Se aprecian sustancias contaminantes o peligrosas sin control?	N/A
4.20.18	¿Se aprecian residuos incontrolados?	N/A
4.20.19	¿Se aprecia suciedad y desorden?	N/A
4.20.20	Si existen objetos de valor ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.20.21	¿Hay detector de humedad y temperatura?	N/A

Observaciones:

4.21 ZONAS DE TRABAJO ADMINISTRATIVO

APLICA | NO

4.21.1	¿Se encuentra la zona administrativa en un recinto delimitado y cerrado?	N/A
4.21.2	¿Permanece cerrada con llave fuera del horario laboral?	N/A
4.21.3	¿Se controla el acceso a la zona administrativa de algún modo?	N/A
4.21.4	¿Se verifica de algún modo, ante la presencia de ajenos (Proveedores, clientes o visitantes), que tengan necesidad de permanecer en este lugar de trabajo?	N/A
4.21.5	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.21.6	¿Cuenta el recinto con detectores de movimiento? ¿o se detecta la apertura de puertas o la posible entrada por ventanas?	N/A
4.21.7	¿Hay documentos sensibles para MAPFRE o con datos personales en las mesas de trabajo, papeleras y estanterías abiertas, posibilitando el acceso por terceros?	N/A
4.21.8	¿Se encuentran las zonas ofimáticas y de valijas fuera del paso o en lugares controlados por la vista de los empleados?	N/A
4.21.9	¿Se arrojan a la papelera documentos sensibles para MAPFRE o que contengan datos personales?	N/A
4.21.10	¿Hay contenedores de papel clasificado?	N/A
4.21.11	¿Hay contenedores para reciclar papel?	N/A
4.21.12	¿Están los contenedores fuera del alcance de ajenos?	N/A
4.21.13	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.21.14	¿Se detecta la presencia de sustancias ó productos inflamables sin control?	N/A
4.21.15	¿Cuenta con extintores adecuados?	N/A
4.21.16	¿Cuenta con detección automática de incendios?	N/A
4.21.17	¿Cuenta con BIES próximas?	N/A
4.21.18	¿Cuenta con iluminación y señalización de emergencia?	N/A
4.21.19	¿Se aprecian residuos incontrolados?	N/A
4.21.20	¿Se aprecian sustancias contaminantes o peligrosas?	N/A
4.21.21	¿Hay destructoras o contenedores de documentos?	N/A
4.21.22	¿Hay cajas fuertes o armarios de seguridad?	N/A
4.21.23	Si existen objeto de valor ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A
4.21.24	¿Se aprecia suciedad y desorden?	N/A
4.21.25	¿Existe contenedor de tóner?	N/A

Observaciones:

4.22 SALA DE REUNIONES (Aulas, sala de juntas, auditorios)

APLICA | NO

4.22.1	¿Permanecen cerradas con llave cuando no están ocupadas?	N/A
4.22.2	¿Se controlan las llaves?	N/A
4.22.3	¿Dificultan la intrusión la estructura y puertas?	N/A
4.22.4	¿Cuenta el recinto con detectores de movimiento? ¿o se detecta la apertura de puertas o la posible entrada por ventanas?	N/A
4.22.5	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.22.6	¿Cuenta con extintores adecuados?	N/A
4.22.7	¿Cuenta con detección automática?	N/A
4.22.8	¿Cuenta con iluminación y señalización de emergencia?	N/A
4.22.9	¿Se aprecian residuos incontrolados?	N/A
4.22.10	¿Se aprecia suciedad o desorden?	N/A
4.22.11	Si existen objeto de valor ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A

Observaciones:

4.23 DESPACHOS DE DIRECCIÓN Y ZONAS SENSIBLES POR MANEJO DE DATOS

APLICA | NO

4.23.1	¿Están vigilados los despachos de dirección?	N/A
4.23.2	¿En la zona o inmediaciones existe circuito cerrado de televisión?	N/A
4.23.3	¿Se controla el acceso permitiéndolo solo a los autorizados?	N/A
4.23.4	¿Permanecen cerrados con llave cuando no están ocupados?	N/A
4.23.5	¿Se controlan las llaves?	N/A
4.23.6	¿Se controla el acceso por medio de tarjeta?	N/A
4.23.7	¿Dificultan la estructura y puertas la intrusión?	N/A
4.23.8	¿Existen detectores de movimiento o detectores de intrusión por ventanas, puertas, etc.)	N/A
4.23.9	¿Existen objetos o equipos que supongan un aumento de la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.23.10	¿Cuenta con extintores adecuados?	N/A
4.23.11	¿Cuenta con detección automática de incendios?	N/A
4.23.12	¿Se aprecian residuos incontrolados?	N/A
4.23.13	¿Hay documentos sensibles para MAPFRE o con datos personales en las mesas de trabajo, papeleras y estanterías abiertas, posibilitando el acceso por terceros?	N/A
4.23.14	¿Se arrojan a la papelera documentos sensibles para MAPFRE o que contengan datos personales?	N/A
4.23.15	¿Hay destructoras o contenedores de documentos?	N/A
4.23.16	¿Hay cajas fuertes o armarios de seguridad?	N/A
4.23.17	Si existen objeto de valor ¿tienen suficientes medidas de protección? (Especifique cuáles en observaciones)	N/A

Observaciones:

4.24 PATINILLOS | APLICA | NO

4.24.1	¿Disponen de puertas cerradas, con cierta consistencia?	N/A
4.24.2	¿Están cerrados los patinillos con llave?	N/A
4.24.3	¿Existen objetos que supongan un incremento a la carga de fuego, o apilaciones mayores a 2 m?	N/A
4.24.4	¿Cuentan con protección contra incendios (PCI) adecuada?	N/A
4.24.5	¿Están sellados y/o sectorizados entre plantas?	N/A
4.24.6	¿Se aprecia suciedad y desorden?	N/A

Observaciones:

5. SISTEMAS Y MEDIOS DE SEGURIDAD Y MEDIO AMBIENTE | APLICA | NO

5.1	¿Están conectados los sistemas electrónicos de seguridad a una central de alarmas o centro de control?	N/A
5.2	¿Están atendidas permanentemente las señales de alarma?	N/A
5.3	¿Está correctamente mantenido El Sistema Electrónico de Seguridad (SES)?	N/A
5.4	¿Esta correctamente dimensionado y en perfecto estado de funcionamiento?	N/A
5.5	¿Capta el sistema, ante la activación de una alarma, la atención del operador hacia ese punto, en todo momento?	N/A
5.6	¿Se recepcionan las señales de incendio en una central atendida permanentemente?	N/A
5.7	¿Existe conexión redundante a más de una central?	N/A
5.8	¿Se gestionan las alarmas de temperatura y humedad de los recintos críticos?	N/A
5.9	¿Está implementado un protocolo para el mantenimiento del sistema de PCI?	N/A
5.10	¿Los medios humanos de seguridad son suficientes?	N/A
5.11	¿Cuenta el personal de seguridad con la titulación y acreditación adecuada de acuerdo a sus cometidos?	N/A
5.12	¿Se adecuan las medidas y medios de seguridad a lo dispuesto en la Normativa de Seguridad Privada (LSP)?	N/A
5.13	¿Se adecuan los sistemas de protección contra incendios a la normativa vigente para este tipo de instalación?	N/A
5.14	¿Funciona la iluminación y señalización de emergencias correctamente?	N/A
5.15	¿Cuenta la instalación con los seguros suficientes para cubrir los riesgos de RC, daños, incendio, robo, etc.?	N/A
5.16	¿Se dispone de un sistema de megafonía y sirenas en perfecto estado de funcionamiento?	N/A
5.17	¿Se dispone de armario cerrado para la custodia de llaves?	N/A
5.18	¿Se observan las directrices de Seguridad de la Información?	N/A
5.19	¿Se dispone de equipo de bombeo para evitar las inundaciones?	N/A
5.20	¿Existe coordinación e intercambio de información con las FCS, tanto a nivel de la DISMA, como a nivel local?	N/A
5.21	¿Se recicla el tóner en el edificio ?	N/A
5.22	¿Se recicla el papel en el edificio?	N/A
5.23	¿Se emplean medios electrónicos para inspección del correo postal y correspondencia?	N/A
5.24	¿El personal que opera el scanner esta debidamente titulado?	N/A
5.25	¿Se dispone de SAI o generadores que garanticen la continuidad de los sistemas ante un corte de suministro?	N/A
5.26	¿Se revisa mediante medios electrónicos la paquetería y correspondencia que llega al edificio?	N/A
5.27	¿Existe y se aplica algún protocolo para trabajos en caliente en el edificio?	N/A
5.28	¿Cuenta el edificio con extinción automática de incendios en aquellos lugares donde debe tenerla por normativa o por el nivel de riesgo que soporta?	N/A
5.29	¿Cierran perfectamente y aíslan suficientemente las ventanas y puertas exteriores del edificio de la temperatura exterior?	N/A
5.30	¿Permite el cierre y la capacidad de aislamiento de las puertas y ventanas mantener la temperatura adecuada en las zonas de trabajo?	N/A
5.31	¿Tiene el edificio algún sistema de sombras, natural o artificial que mitiga el sobrecalentamiento en verano?	N/A
5.32	¿Es necesario mantener encendida la luz artificial en las zonas de trabajo durante toda la jornada laboral?	N/A
5.33	¿Está sectorizado el edificio en zonas en función de la energía que demandan?	N/A
5.34	¿Se utilizan calderas de gas natural y no de otros combustibles fósiles?	N/A
5.35	¿Son los equipos de producción de frío de alto rendimiento?	N/A
5.36	¿Se utilizan temporizadores o detectores de presencia para la iluminación de las zonas de paso?	N/A
5.37	¿Es accionable la iluminación de las zonas de aparcamiento con pulsador junto a la puerta?	N/A
5.38	¿Se emplean válvulas y dispositivos de ahorro de agua en las instalaciones sanitarias del edificio?	N/A
5.39	¿Se realiza mantenimiento preventivo y correctivo oportuno para minimizar las pérdidas por fugas de agua en las instalaciones sanitarias del edificio?	N/A
5.40	¿Se mantienen adecuadamente los cuadros eléctricos de todo el edificio o de elementos que puedan provocar un incendio?	N/A
5.41	¿Se realiza la detección de posibles puntos calientes?	N/A
5.42	¿Se realizan los mantenimientos adecuados a los sistemas de seguridad y PCI?	N/A
5.43	¿Está prohibido fumar?	N/A
5.44	¿Se gestionan los aljibes y torres de refrigeración conforme al protocolo de medio ambiente?	N/A
5.45	¿Se mantienen adecuadamente los ascensores y la maquinaria del edificio?	N/A
5.46	¿Dispone de equipos para inspección postal o de paquetería en el edificio (Scanner)?	N/A
5.47	¿Las bombillas tienen protección contra incendio?	N/A

Observaciones:

6. HISTÓRICO DE INCIDENTES	APLICA	NO

6.1 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.2 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.3 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.4 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.5 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.6 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.7 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

6.8 Riesgo afectado:	Seleccione...	Gravedad	Seleccione...

Observaciones:

ANEXO III: Algoritmo para establecer la relación de los riesgos con la situación identificada mediante los ítems contestados. Incluye la valoración cualitativa de los posibles riesgos. (Extracto)

1. RELACION DE AMENAZAS Y VULNERABILIDADES (Extracto)

INCLUSIÓN DE TEXTOS EN FUNCIÓN DE LAS CARACTERÍSTICAS Y DE LOS RIESGOS GLOBALES DETECTADOS

AMENAZAS Y VULNERABILIDADES
Museo.
En un museo el riesgo de robo se incrementa notablemente. Dado el valor de los activos que contiene debe considerarse incluso el robo profesional. La afluencia de público incrementa el riesgo de daños a terceros. Estos establecimientos deben contar con unas medidas de seguridad y contra incendios específicas y acordes con la normativa.
Aulas de formación.
Hay que tener en cuenta un posible incremento de hurtos y las disposiciones normativas específicas sobre protección de incendios. De igual forma, puede elevarse el riesgo de daños a terceros
Centro comercial.
La afluencia de público ajeno a MAPFRE junto a la presencia de establecimientos de naturaleza diferente que se ubican en un centro comercial, implican la posibilidad de ciertos riesgos o el incremento de otros. Así cabe mencionar el de hurto y robo, daños a terceros e incendio. También hay que destacar el posible riesgo de incumplimiento derivado de la normativa específica en cuanto a las protecciones contra incendios obligatorias, así como el derivado de los requerimientos normativos sobre la gestión de emergencias y planes de autoprotección.
Centro del Automóvil (PPR).
En los PPR se cuenta con los riesgos derivados de la gestión de datos personales, LOPD. Se puede incrementar o reducir este riesgo en función de la disposición o no de las medidas de seguridad y organizativas oportunas.
Centro médico.
En un centro médico se ha de considerar de forma especial el riesgo de incumplimiento de la LOPD y su normativa de desarrollo, en la medida en que se custodien documentos con datos personales sin las medidas de seguridad pertinentes. Una inadecuada gestión de residuos puede derivar en riesgo medioambiental. Se ha de atender al riesgo de daños a terceros, considerando que se trata de locales abiertos al público.
Complejo de varios edificios.
El hecho de que se trate de un complejo de varios edificios influye en los riesgos soportados, teniendo en cuenta que se tratará de un inmueble de mayor magnitud, con mayor número de ocupantes, de externos, proveedores, y visitas en general, así como su mayor representatividad. Estos factores operan como potenciadores de los riesgos analizados en general, con particular incidencia en los de intrusión, imagen, hurtos y seguridad de la información. Por el contrario como reductores del riesgo hay que mencionar que, generalmente, cuentan con controles de accesos muy protocolizados y frecuentemente redundantes, así como con equipos específicos para tareas como mantenimiento. La categoría y presencia de estos complejos con medidas de seguridad visibles opera como factor disuasorio, reduciendo globalmente los riesgos.
Edificio aislado.
El hecho de tratarse de un edificio aislado puede incrementar el nivel de riesgos como la intrusión y los derivados de la misma, considerando la posibilidad de ocultamiento y la mayor dificultad para reaccionar. Es posible que se incremente el riesgo de incendio por una mayor dificultad para su detección.

.....

Edificio directo a la vía.
Se considera que el hecho de que se trate de un edificio al que se accede directamente desde la vía incrementa la posibilidad de que ajenos intenten acceder al mismo, incrementando la posibilidad del riesgo de intrusión y los posibilitados a partir de la misma. La presencia de viandantes en las inmediaciones del edificio y la de edificios ajenos en el entorno próximo, incrementa los riesgos de daños a terceros.
Edificio próximo a autopista con posibles riesgos asociados sin control.
La proximidad de la instalación a una autopista o vía de alta densidad de tráfico, puede implicar los riesgos que se mencionan, entre otros, y cuya identificación y valoración deben efectuarse de forma específica: Riesgo de daños a las personas. Facilidad para el escape ante un delito contra la instalación o sus personas. Riesgos que afecten al funcionamiento de la instalación, en particular a los accesos y a los equipos. Riesgo por vertido de producto contaminante que se transportase. Riesgo por efectos de una accidente de tráfico
En zona con altas precipitaciones sin protección y medios de seguridad exigidos legal y/o técnicamente.
Si se presentan grandes precipitaciones en periodos relativamente cortos o precipitaciones persistentes que aumenten representativamente el nivel de los cuerpos de agua. También puede generar remociones de masa que afecten edificaciones o represen flujos de agua. En aquel caso en que la carga de agua supera la capacidad normal de evacuación de los causes genera inundaciones que pueden afectar parcialmente las instalaciones de edificios, causando daño a equipos eléctricos, electrónicos, o archivos.
En zona con actividad volcánica sin protección y medios de seguridad exigidos legal y/o técnicamente.
Las edificaciones localizadas en la zona de influencia de un volcán activo, pueden estar sometidas a distintos tipo de erupción que incluyen la expulsión de ceniza abrasiva, la explusión de lava, con explosión de gases a elevadas presiones y temperatura. Estás explosiones pueden estar acompañadas de avalanchas o aludes.

.....

2. ASOCIACIÓN DE LOS ÍTEMS CON LOS RIESGOS DERIVADOS DEL ENTORNO (RIESGOS GLOBALES)

2.1	Riesgo Asociado a: Complejo de varios edificios	El hecho de que se trate de un complejo de varios edificios influye en los riesgos soportados, teniendo en cuenta que se tratará de un inmueble de mayor magnitud, con mayor número de ocupantes, de externos, proveedores, y visitas en general, así como su mayor representatividad. Estos factores operan como potenciadores de los riesgos analizados en general, con particular incidencia en los de intrusión, imagen, hurtos y seguridad de la información. Por el contrario como reductores del riesgo hay que mencionar que, generalmente, cuentan con controles de accesos muy protocolizados y frecuentemente redundantes, así como con equipos específicos para tareas como mantenimiento. La categoría y presencia de estos complejos con medidas de seguridad visibles opera como factor disuasorio, reduciendo globalmente los riesgos.
2.2	Riesgo Asociado a: Edificio directo a la vía	Se considera que el hecho de que se trate de un edificio al que se accede directamente desde la vía incrementa la posibilidad de que ajenos intenten acceder al mismo, incrementando la posibilidad del riesgo de intrusión y los posibilitados a partir de la misma. La presencia de viandantes en las inmediaciones del edificio y la de edificios ajenos en el entorno próximo, incrementa los riesgos de daños a terceros.
2.3	Riesgo Asociado a: Edificio aislado	El hecho de tratarse de un edificio aislado puede incrementar el nivel de riesgos como la intrusión y los derivados de la misma, considerando la posibilidad de ocultamiento y la mayor dificultad para reaccionar. Es posible que se incremente el riesgo de incendio por una mayor dificultad para su detección.
2.4	Riesgo Asociado a: Edificio con parcela y valla	El hecho de disponer de vallado opera como reductor de todos los riesgos asociados a la intrusión, particularmente si se combina con un control de accesos exterior en el propio vallado y este se encuentra en buen estado, y dotado de las medidas de seguridad oportunas. Una valla en malas condiciones puede afectar en sentido contrario dando imagen de escaso interés por la seguridad, afectando además a la imagen de la empresa en general. Deben considerarse posibles riesgos medio ambientales asociados a la parcela, en función de la vegetación que se encuentre en ésta y de otros aspectos que se identifiquen.
2.5	Riesgo Asociado a: Edificio con parcela sin valla	El hecho de tener parcela sin vallado, no favorece la seguridad de la instalación. Si además posibilita el ocultamiento, se incrementa el riesgo de intrusión y los asociados a este. El incendio y el riesgo medioambiental pueden incrementarse si está descuidada en cuanto a vegetación. Con esto también se proyectaría una mala imagen.
2.12	Riesgo Asociado a: Museo	En un museo el riesgo de robo se incrementa notablemente. Dado el valor de los activos que contiene debe considerarse incluso el robo profesional. La afluencia de público incrementa el riesgo de daños a terceros. Estos establecimientos deben contar con unas medidas de seguridad y contra incendios específicas y acordes con la normativa.
2.13	Riesgo Asociado a: Aulas de formación	Hay que tener en cuenta un posible incremento de hurtos y las disposiciones normativas específicas sobre protección de incendios. De igual forma, puede elevarse el riesgo de daños a terceros
2.14	Riesgo Asociado a: Centro del Automóvil (PPR)	En los PPR se cuenta con los riesgos derivados de la gestión de datos personales, LOPD. Se puede incrementar o reducir este riesgo en función de la disposición o no de las medidas de seguridad y organizativas oportunas.
2.15	Riesgo Asociado a: Centro comercial	La afluencia de público ajeno a MAPFRE junto a la presencia de establecimientos de naturaleza diferente que se ubican en un centro comercial, implican la posibilidad de ciertos riesgos o el incremento de otros. Así cabe mencionar el de hurto y robo, daños a terceros e incendio. También hay que destacar el posible riesgo de incumplimiento derivado de la normativa específica en cuanto a las protecciones contra incendios obligatorias, así como el derivado de los requerimientos normativos sobre la gestión de emergencias y planes de autoprotección.
2.16	Riesgo Asociado a: Centro médico	En un centro médico se ha de considerar de forma especial el riesgo de incumplimiento de la LOPD y su normativa de desarrollo, en la medida en que se custodien documentos con datos personales sin las medidas de seguridad pertinentes. Una inadecuada gestión de residuos puede derivar en riesgo medioambiental. Se ha de atender al riesgo de daños a terceros, considerando que se trata de locales abiertos al público

•••••

3.17	Riesgo Asociado a: En zona con actividad volcánica sin protección y medios de seguridad exigidos legal y/o técnicamente.	Las edificaciones localizadas en la zona de influencia de un volcán activo, pueden estar sometidas a distintos tipo de erupción que incluyen la expulsión de ceniza abrasiva, la explusión de lava, con explosión de gases a elevadas presiones y temperatura. Estás explosiones pueden estar acompañadas de avalanchas o aludes. Para tratar este riesgo, es necesario tener planes de contingencia, evacuación, continuidad de negocio, protección de bienes, equipos, documentos, personas, etc.	NO
3.18	Riesgo Asociado a: En zona con altas precipitaciones sin protección y medios de seguridad exigidos legal y/o técnicamente.	Si se presentan grandes precipitaciones en periodos relativamente cortos o precipitaciones persistentes que aumenten representativamente el nivel de los cuerpos de agua. También puede generar remociones de masa que afecten edificaciones o represen flujos de agua. En aquel caso en que la carga de agua supera la capacidad normal de evacuación de los causes genera inundaciones que pueden afectar parcialmente las instalaciones de edificios, causando daño a equipos eléctricos, electrónicos, o archivos.	NO
3.19	Riesgo Asociado a: En zona donde se presentan vientos fuertes sin protección y medios de seguridad exigidos legal y/o técnicamente.	En el caso de presentarse vientos extremos, súbitos, de alta velocidad y duración, pueden afectarse techos, instalaciones de comunicación, redes eléctricas aéreas, ocurrir caida de árboles, impacto de elementos contundentes en ventanas, lesiones personales, daños en el contenido de edificios o en parqueaderos, etc. Para tratar el riesgo se deben evaluar las coberturas de los seguros para la reposición de bienes y para atender los casos de responsabilidad civil.	NO
3.26	Riesgo Asociado a: En zona con amenaza o vulnerabilidad terrorista sin protección y medios de seguridad para controlar el riesgo	Sobre esta instalación, personal de la misma, o en general sobre la zona o el entorno en que se encuentra, pende amenaza terrorista. Este riesgo grave exige que se incrementen los controles establecidos, en particular los accesos y las medidas de autoprotección y protección personales. De forma especial, deberá incrementarse la colaboración con las FSE.	NO
3.27	Riesgo Asociado a: Hay empresas o actividades próximas que puedan generar daños a la instalación o a sus ocupantes, y no se tienen medidas de protección y medios de seguridad para controlar el riesgo	La proximidad de la instalación a empresas potencialmente peligrosas, puede implicar los riesgos que se mencionan, entre otros, y cuya identificación y valoración deben efectuarse de forma específica, debiendo en función de los mismos adoptar las medidas de coordinación necesarias con esa empresa: Riesgo de daños a las personas. Riesgos que afecten al funcionamiento de la instalación, en particular a los accesos y a los equipos. Ruido. Riesgo de Incendio o explosión.	NO
3.28	Riesgo Asociado a: Entorno social o delincuencialmente conflictivo, , y no se tienen medidas de protección y medios de seguridad para controlar el riesgo	La proximidad de la instalación a una zona delincuencialmente peligrosa, o máxime si se encuentra ubicada dentro de la misma zona, , puede implicar los riesgos que se mencionan, entre otros, y cuya identificación y valoración deben efectuarse de forma específica, debiendo en función de los mismos adoptar las medidas de control necesarias: Riesgo de daños a las personas. Riesgos de robo, hurto, atraco. Riesgo de Agresiones. Riesgo de daños en general. Riesgo de vandalismo.	NO
3.29	Riesgo Asociado a: La instalación no cuenta con Pararrayos	En el caso de presentarse tormentas eléctricas y al no tener pararrayos, pueden afectarse los sistemas eléctricos y electrónicos del edificio y ocasionar daños a los equipos y sistemas que contienen información o realizan transacciones, así mismo puede causar traumatismos en los accesos y salidas automáticas. Para tratar el riesgo se deben evaluar las coberturas de los seguros para la reposición de bienes y para atender los casos de responsabilidad civil. De igual manera se debe gestionar la instalación de pararrayos.	SI
3.30	Riesgo Asociado a: Distancia de los Bomberos	Cuando la distancia a los bomberos excede los 10 minutos se incrementa el riesgo y se hace necesario que los sistemas de protección contra incendios estén en buen funcionamiento y ayuden a lograr contener el incendio mientras que accede al lugar el carro de bomberos.	SI
3.37	Riesgo Asociado a: Plan de seguridad	Cuando no se tiene o no se aplica un plan de seguridad se hace evidente una vulnerabilidad y se incrementa la amenaza que el riesgo pueda materializarse, por lo que para tratar el riesgo se debe garantizar que se tenga un plan de seguridad, que todos los funcionarios lo conocen y que se encuentre implementado.	SI

Para cada riesgo se señalan las preguntas (identificadas por su número del Check List) que le afectan o lo posibilitan, con expresión del grado de riesgo, asociando de esta forma también los riesgos a las zonas donde concretamente se han detectado las situaciones o factores de riesgo.

Se establecen 2.552 relaciones de riesgo.

AGRESIONES										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDAD
3.37	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.15	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.16	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.4.6	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.4.10	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.6.1	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.6.2	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.6.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.6.4	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.7.14	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.15.1	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.15.2	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.15.3	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.15.5	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.15.6	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.16.1	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.16.2	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.16.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.17.3	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.17.4	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.17.5	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.17.6	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA

.....

ROBO-HURTO-ATRACO										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDAD
3.28	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.37	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.41	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.1	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.2	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.4	NO	N/A	BAJO	0		0	0	0	0	NO APLICA

.....

INTRUSION

Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.28	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.37	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.1	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.2	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.3	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.4	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.5	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.6	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.7	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.8	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.9	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.10	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.11	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.12	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
4.1.13	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.14	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.15	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.16	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.17	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.1	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.2	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.3	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
4.2.4	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.5	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
4.2.6	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.13	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.14	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
4.2.15	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.20	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.3.1	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA

SABOTAJE

Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.41	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.1	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.2	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.5	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.15	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.16	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.17	NO	N/A	BAJO	0		0	0	0	0	NO APLICA

.....

VANDALISMO

Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
4.1.1	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.5	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.6	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.7	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.8	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.9	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.10	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.11	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.12	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.1	NO	N/A	BAJO	0		0	0	0	0	NO APLICA

.....

TERRORISMO

Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.26	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
4.7.9	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.7.10	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.7.13	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.8.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.16.2	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.16.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.20.1	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA

.....

CONTAMINACIÓN GENERAL (MEDIO AMBIENTAL)

Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
4.2	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.12	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.13	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.3.15	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.3.18	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.3.19	SI	N/A	ALTO	0		0	0	0	0	NO APLICA
4.3.20	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.5.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.5.8	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.5.11	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.6.16	SI	N/A	BAJO	0		0	0	0	0	NO APLICA
4.6.23	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.6.25	SI	N/A	ALTO	0		0	0	0	0	NO APLICA
4.6.26	SI	N/A	ALTO	0		0	0	0	0	NO APLICA
4.7.27	SI	N/A	BAJO	0		0	0	0	0	NO APLICA

.....

INCUMPLIMIENTO DE LA NORMATIVA DE PROTECCION DE DATOS										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.41	NO	N/A	ALTO	0		0	0	0	0	NO APLICA

.....

INCUMPLIMIENTO NORMATIVA PCI/ ATP										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.40	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
3.45	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.14	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA

.....

INCENDIO										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.5	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
3.11	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.12	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.13	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.17	NO	N/A	ALTO	0		0	0	0	0	NO APLICA
3.29	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
3.30	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
3.40	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.7	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.8	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.9	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.10	SI	N/A	ALTO	0		0	0	0	0	NO APLICA

.....

DAÑOS O PÉRDIDA DE INFORMACIÓN										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.37	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
3.40	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
3.41	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.1.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.10	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.12	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.15	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.16	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.1.17	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.1	NO	N/A	BAJO	0		0	0	0	0	NO APLICA

.....

IMAGEN										
Pregunta	Aum. Dism. Riesgo	Respuesta	Nivel Riesgo	ALTO		MEDIO		BAJO		CONTEO INTENSIDA
3.39	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
3.40	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.1	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.3	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.5	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.11	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.12	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.13	SI	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.14	NO	N/A	BAJO	0		0	0	0	0	NO APLICA
4.2.15	NO	N/A	MEDIO	0		0	0	0	0	NO APLICA
4.2.16	NO	N/A	BAJO	0		0	0	0	0	NO APLICA

.....

CONSECUTIVO AHORA	RIESGOS	VALOR	RIESGO ALTO	RIESGO MEDIO	RIESGO BAJO	VALOR GLOBAL DEL RIESGO (VGR) INSTALACIÓN (Obtenido
1	AGRESIONES	0,000	0	0	0	
2	ROBO-HURTO	0,000	0	0	0	
3	INTRUSIÓN	0,000	0	0	0	
4	SABOTAJE	0,000	0	0	0	
5	VANDALISMO	0,000	0	0	0	
6	TERRORISMO	0,000	0	0	0	
7	NATURALEZA	0,000	0	0	0	
8	INUNDACIÓN	0,000	0	0	0	
9	CONTAMINACIÓN GENERAL (MEDIO AMBIENTAL)	0,000	0	0	0	
10	BIOLÓGICO	0,000	0	0	0	
11	CONSUMOS INDISCRIMINADOS O EXCESIVOS	0,000	0	0	0	
12	INCUMPLIMIENTO DE LA NORMATIVA DE PROTECCION DE DATOS	0,000	0	0	0	
13	INCUMPLIMIENTO DE NORMATIVA MEDIO AMBIENTAL	0,000	0	0	0	
14	INCUMPLIMIENTO DE LA NORMATIVA DE LA PROTECCION CONTRA INCENDIOS Y PLANES DE AUTOPROTECCION	0,000	0	0	0	
15	OTROS POSIBLES INCUMPLIMIENTOS NORMATIVOS	0,000	0	0	0	
16	INCENDIO	0,000	0	0	0	
17	RIESGO LABORAL	0,000	0	0	0	
18	DAÑOS - RESPONSABILIDAD CIVIL (RC)	0,000	0	0	0	
19	DAÑOS O PÉRDIDAD DE INFORMACIÓN (seguridad de la	0,000	0	0	0	
20	IMAGEN	0,000	0	0	0	
21	CONTINUIDAD DE NEGOCIO (CN)	0,000	0	0	0	
	VALOR GLOBAL DEL RIESGO EN INSTALACIÓN (VGR)	0,000				0

Pregunt	Atún. Dism. Riesgo	Respues	Nivel Ries	ALTO	MEDIO	BAJO	RESPUESTAS	VALIDACI	ZONAS
3.37	NO	N/A	BAJO	0	0	0	No conoce y aplica un plan de seguridad específico para la edificación.	N/A	RIESGOS GLOBALES
4.2.15	NO	N/A	MEDIO	0	0	0	En el (CC/SS) no se aplica un protocolo de actuación para controlar el acceso de vehículos a la instalación.	N/A	CUARTO DE CONTROL SALA SEGURIDAD
4.2.16	NO	N/A	MEDIO	0	0	0	En el (CC/SS) no se aplica un protocolo de actuación para controlar el acceso de peatones a la instalación.	N/A	CUARTO DE CONTROL SALA SEGURIDAD
4.4.6	NO	N/A	BAJO	0	0	0	La puerta principal no se cierra tras finalizar la jornada laboral.	N/A	FACHADA Y ESTRUCTURA PARTE INTERIOF
4.4.10	NO	N/A	BAJO	0	0	0	Las puertas secundarias no permanecen habitualmente cerradas y permiten el paso a cualquier persona.	N/A	FACHADA Y ESTRUCTURA PARTE INTERIOF
4.6.1	NO	N/A	MEDIO	0	0	0	En la oficina directa no está vigilado el acceso exterior.	N/A	OFICINA DIRECTA
4.6.2	NO	N/A	BAJO	0	0	0	En la zona y/o inmediaciones no existe circuito cerrado de televisión.	N/A	OFICINA DIRECTA
4.6.3	NO	N/A	BAJO	0	0	0	La estructura y puertas no dificultan la intrusión en la oficina directa.	N/A	OFICINA DIRECTA
4.6.4	NO	N/A	MEDIO	0	0	0	No se controla el cierre y apertura de puertas (interior y exterior) de la oficina directa.	N/A	OFICINA DIRECTA
4.7.14	NO	N/A	BAJO	0	0	0	El acceso desde el parking al interior del edificio no se controla.	N/A	PARKING
4.15.1	NO	N/A	BAJO	0	0	0	El Hall no se controla el acceso de ajenos.	N/A	HALL
4.15.2	NO	N/A	BAJO	0	0	0	En la zona y/o inmediaciones no existe circuito cerrado de televisión.	N/A	HALL
[illegible]	[illegible]	[illegible]	[illegible]	0	0	0	El hall de la planta baja (PB) no está vigilado por medios	N/A	[illegible]

. . . . . .

[illegible]	[illegible]	[illegible]	[illegible]	0	0	0	La valla no está en buen estado de mantenimiento.	N/A	VALLADO
4.1.4	NO	N/A	BAJO	0	0	0	La valla no está securizada o no detecta un intento de vulnerarla.	N/A	VALLADO
4.1.5	NO	N/A	BAJO	0	0	0	La valla no dificulta la escalada.	N/A	VALLADO
4.1.6	NO	N/A	BAJO	0	0	0	La valla no está vigilada por ningún medio.	N/A	VALLADO
4.1.7	NO	N/A	BAJO	0	0	0	La valla no está vigilada mediante circuito cerrado de televisión.	N/A	VALLADO
4.1.8	NO	N/A	BAJO	0	0	0	La iluminación de la valla no suficiente.	N/A	VALLADO
4.1.9	NO	N/A	BAJO	0	0	0	La valla no cuenta con iluminación sorpresiva.	N/A	VALLADO
4.1.10	NO	N/A	MEDIO	0	0	0	Las puertas de acceso del vallado no se cierran fuera del horario laboral.	N/A	VALLADO

. . . . . .

4.14.1	NO	N/A	BAJO	0	0	0	[illegible] por ningún medio.	N/A	ARCHIVOS SALA DE COMUNICACIONES, CF
4.14.2	NO	N/A	BAJO	0	0	0	No se capta el acceso a los Archivos, CPD o sala de comunicaciones mediante circuito cerrado de televisión.	N/A	ARCHIVOS SALA DE COMUNICACIONES, CF
4.14.3	NO	N/A	MEDIO	0	0	0	Los CPD o sala de comunicaciones habitualmente no están cerrados impidiendo el libre acceso.	N/A	ARCHIVOS SALA DE COMUNICACIONES, CF
4.14.4	NO	N/A	BAJO	0	0	0	Los Archivos, CPD o sala de comunicaciones no cuentan con detección de movimiento.	N/A	ARCHIVOS SALA DE COMUNICACIONES, CF

4.21.3	NO	N/A	BAJO	0	0	0	No se controla de ningún modo el acceso a la zona administrativa.	N/A	ZONAS DE TRABAJO ADMINISTRATIVA
4.21.4	NO	N/A	BAJO	0	0	0	Ante la presencia de ajenos (Proveedores, clientes o visitantes), no se verifica de ningún modo que tengan necesidad de permanecer en esta zona administrativa.	N/A	ZONAS DE TRABAJO ADMINISTRATIVA
4.21.5	NO	N/A	BAJO	0	0	0	En la zona y/o inmediaciones no existe circuito cerrado de televisión.	N/A	ZONAS DE TRABAJO ADMINISTRATIVA

4.23.18	NO	N/A	MEDIO	0	0	0	En los despachos de dirección o en los que se maneja documentación sensible no hay cajas fuertes o armarios de seguridad.	N/A	DESPACHOS DE DIRECCIÓN
4.23.19	NO	N/A	MEDIO	0	0	0	En los despachos de dirección o en los que se maneja documentación sensible existen objetos de valor sin suficientes medidas de protección.	N/A	DESPACHOS DE DIRECCIÓN
5.1	NO	N/A	MEDIO	0	0	0	Los sistemas electrónicos de seguridad no están conectados a una central de alarmas o centro de control.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y ME

4.1.16	NO	N/A	MEDIO	0	0	0	En el vallado el acceso principal y/o el de uso habitual no cuentan con tornos o medios para el control de peatones.	N/A	VALLADO
4.1.17	NO	N/A	BAJO	0	0	0	El vallado no dispone de interfono.	N/A	VALLADO
4.2.1	NO	N/A	MEDIO	0	0	0	No se vigila por algún medio la zona de acceso al centro de control por ningún medio.	N/A	CUARTO DE CONTROL SALA SEGURIDAD
4.2.2	NO	N/A	BAJO	0	0	0	No se vigila mediante circuito cerrado de televisión el centro de control.	N/A	CUARTO DE CONTROL SALA SEGURIDAD
4.2.3	NO	N/A	ALTO	0	0	0	No se controla el acceso al interior del Centro de control (CC/SS) o no se restringe al personal autorizado.	N/A	CUARTO DE CONTROL SALA SEGURIDAD

4.7.8	NO	N/A	BAJO	0	0	0	No se verifica que los vehículos estacionados en el parking están autorizados para ocupar esa plaza.	N/A	PARKING
4.7.9	NO	N/A	BAJO	0	0	0	El parking no permanece cerrado fuera del horario laboral.	N/A	PARKING
4.7.10	NO	N/A	BAJO	0	0	0	No se realiza control de vehículos que permanecen en el parking fuera del horario laboral.	N/A	PARKING
4.7.11	NO	N/A	BAJO	0	0	0	Las puertas del parking no son resistentes.	N/A	PARKING

4.17.4	NO	N/A	MEDIO	0	0	0	Las salidas de emergencia no están habitualmente cerradas.	N/A	SALIDAS DE EMERGENCIA
4.17.5	NO	N/A	MEDIO	0	0	0	Las salidas de emergencia no tienen detector de apertura.	N/A	SALIDAS DE EMERGENCIA
4.17.6	NO	N/A	BAJO	0	0	0	En las salidas de emergencia no se vigila por algún medio el acceso a las salidas de emergencia.	N/A	SALIDAS DE EMERGENCIA
4.17.7	NO	N/A	BAJO	0	0	0	Las salidas de emergencia no tienen aviso de "Solo abrirse en caso de Emergencia"	N/A	SALIDAS DE EMERGENCIA
4.18.1	NO	N/A	MEDIO	0	0	0	En la cocina no están vigilados los accesos	N/A	COCINA Y CAFETERÍA
4.18.2	NO	N/A	MEDIO	0	0	0	En la zona y/o inmediaciones no existe circuito cerrado de televisión.	N/A	COCINA Y CAFETERÍA

2244	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	atención del operador hacia ese punto, en todo momento.	[illegible]	[illegible]
2245	5.6	NO	N/A	MEDIO	0	0	0	Las señales de incendio no se recepcionan en una central atendida permanentemente.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2246	5.7	NO	N/A	BAJO	0	0	0	No existe conexión redundante a más de una central del sistema de seguridad.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2247	5.8	NO	N/A	BAJO	0	0	0	No se gestionan las alarmas de temperatura y humedad de los recintos críticos.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2248	5.15	NO	N/A	MEDIO	0	0	0	La instalación no cuenta con los seguros suficientes para cubrir los riesgos de RC, daños, incendio, robo, etc.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2249	5.19	NO	N/A	BAJO	0	0	0	No se dispone de equipo de bombeo para evitar las inundaciones.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2250	5.26	NO	N/A	ALTO	0	0	0	En el edificio no se dispone de un equipo de alimentación ininterrumpido que garantice el funcionamiento de los equipos ante un corte de suministro.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2251	5.28	NO	N/A	MEDIO	0	0	0	En el edificio no existe ni se aplica protocolo para trabajos en caliente.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2252	5.29	NO	N/A	MEDIO	0	0	0	El edificio no cuenta con extinción automática de incendios en aquellos lugares donde debe tenerla por normativa o el nivel de riesgo que soporta.	N/A	SISTEMAS Y MEDIOS DE SEGURIDAD Y M
2253	0	0	0	0	0	0	0	0	N/A	#N/A

ANEXO IV: Modelo para informe de análisis de riesgos (Extracto)

	ALTO	MEDIO	BAJO
Agresiones -.			
Ascensores			
El acceso de los proveedores por el ascensor no esta controlado.			
Se accede libremente a los ascensores desde cualquier planta.			
Clínica Consulta Medica			
En la clínica no se controla el acceso.			
En la zona y/o inmediaciones no existe circuito cerrado de televisión.			
La clínica no está vigilada de ninguna forma.			
Cuarto De Control Sala Seguridad			
En el (CC/SS) no se aplica un protocolo de actuación para controlar el acceso de peatones a la instalación.			
En el (CC/SS) no se aplica un protocolo de actuación para controlar el acceso de vehículos a la instalación.			
La zona administrativa no se encuentra en un recinto delimitado y cerrado.			
Biológico -.			
Clínica Consulta Medica			
En la clínica los residuos no se gestionan adecuadamente.			
En la clínica se aprecian sustancias contaminantes o peligrosas.			
Cocina Y Cafetería			
En la cocina existen conducciones ó depósitos de agua que pueden provocar una inundación (elementos que no sean propios de la instalación, en mal estado o que por sus características sea posible su rotura).			
En la cocina se aprecian residuos incontrolados.			
En la cocina se aprecian sustancias contaminantes o peligrosas.			
Correos			
En la zona de correos se aprecian sustancias contaminantes o peligrosas sin control.			
Cuartos Técnicos			
Las baterías en desuso (UPS) no se gestionan conforme al protocolo de medio ambiente.			
Fosa Séptica			
El vaciado o vertido de la fosa ó depuradora no se realiza de acuerdo con el protocolo establecido por Medio Ambiente.			
En los cuartos técnicos se aprecian residuos incontrolados.			
En los cuartos técnicos se aprecian sustancias contaminantes o peligrosas.			
Las baterías en desuso (UPS) no se gestionan conforme al protocolo de medio ambiente.			
No disponen los cuartos de ventilación adecuada.			
Depósito De Combustible			
Daños O Pérdida De Información (Seguridad De La Información) -.			
Archivos Sala De Comunicaciones, Cpd			
El archivo se comparte entre varias entidades y no existen ni se aplican protocolos de uso.			
En los Archivos, CPD o sala de comunicaciones el control de accesos no es mediante tarjeta.			
En la zona de correos las valijas, correspondencia y/o casilleros de correos son fácilmente accesibles para ajenos al servicio.			
En la zona de correos no en todo momento, ni durante la fase de recogida y salida de correos, valija y paquetería se encuentran en un lugar seguro y controlado.			
En la zona de correos no se aplica un protocolo de entrega de paquetería que permita documentar dicha entrega.			
En la zona de correos se detecta la presencia de productos inflamables sin control.			
En la zona y/o inmediaciones no existe circuito cerrado de televisión.			
La zona de correos no cuenta con BIES próximas.			
La zona de correos no cuenta con detección de apertura de puertas.			

Imagen -.			
Almacén			
En el almacén se aprecian residuos incontrolados			
Archivos Sala De Comunicaciones, Cpd			
En los Archivos, CPD o sala de comunicaciones el control de accesos no es mediante tarjeta.			
En los Archivos, CPD o sala de comunicaciones la estructura no es segura, no dificulta o impide la intrusión.			
En los Archivos, CPD o sala de comunicaciones no está prohibido fumar.			
En los Archivos, CPD o sala de comunicaciones no se controla el acceso.			
En los Archivos, CPD o sala de comunicaciones no se cuenta con detección automática de incendios.			

.....

Incendio -.			
Almacén			
El almacén no cuenta con detección automática de incendios.			
El almacén no dispone de extintores adecuados.			
El almacén no está cerrado con llave habitualmente.			
En el almacén se aprecian residuos incontrolados			
En el almacén existen objetos o equipos que supongan un incremento en la carga de fuego o apilaciones mayores de 2 m.			
En el almacén no está prohibido fumar.			
La zona de los almacenes no está vigilada por ningún medio.			

En los Archivos, CPD o sala de comunicaciones se aprecian residuos incontrolados.			
En los Archivos, CPD o sala de comunicaciones se detecta la presencia de productos inflamables sin control.			
En los Archivos, CPD o sala de comunicaciones se detecta la presencia de productos, equipos o elementos que pueden provocar una ignición.			

.....

Incumplimiento De La Normativa De Proteccion De Datos -.			
Archivos Sala De Comunicaciones, Cpd			
En los Archivos, CPD o sala de comunicaciones existen conducciones o depósitos de agua que puedan provocar una inundación o daños a la documentación. (elementos en mal estado o que por sus características sea posible su rotura).			
En los Archivos, CPD o sala de comunicaciones existen objetos, equipos o apilaciones mayores a 2 m que incrementan la carga de fuego.			
En los Archivos, CPD o sala de comunicaciones la estructura no es segura, no dificulta o impide la intrusión.			
En los Archivos, CPD o sala de comunicaciones no se aplica ningún criterio para archivo de la documentación.			
En los Archivos, CPD o sala de comunicaciones no se controla el acceso.			

Despachos De Dirección			
En los despachos de dirección se arrojan a la papelera documentos sensibles para MAPFRE o que contengan datos personales.			
En la zona y/o inmediaciones no existe circuito cerrado de televisión.			
En los despachos de dirección o en los que se maneja documentación sensible la estructura y puertas no dificultan la intrusión.			
En los despachos de dirección o en los que se maneja documentación sensible no hay cajas fuertes o armarios de seguridad.			
En los despachos de dirección o en los que se maneja documentación sensible no se controla el acceso permitiéndolo solo a los autorizados.			

.....

Intrusión -.			
Almacén			
El almacén no está cerrado con llave habitualmente.			

Clínica Consulta Medica			
En la clínica existen objetos de valor sin suficientes medidas de protección.			
En la clínica fuera del horario de atención a pacientes no se controla el acceso por medio de tarjeta.			

Parcela			
En la parcela el acceso de peatones al parking no está controlado.			
En la parcela existen objetos, equipos, materiales o productos que incrementan la carga de fuego.			
En la Parcela los accesos al o desde el parking se no encuentran señalizados.			

.....

Naturaleza -.			
Archivos Sala De Comunicaciones, Cpd			
En los archivos no se controla la aparición de plagas, roedores, insectos, etc.			

.....

Robo-Hurto-Atraco -.			
Almacén			
El almacén no está cerrado con llave habitualmente.			
En el almacén existen objetos de valor sin suficientes medidas de protección.			

En la cocina no se cierran con llave las dependencias y armarios interiores.			
En la zona y/o inmediaciones no existe circuito cerrado de televisión.			
La cocina cuenta con detectores de movimiento.			

En la Planta Baja no se controla el personal que accede al edificio.			
En la zona y/o inmediaciones no existe circuito cerrado de televisión.			
Existen en la zona del hall objetos de especial valor.			

.....

Terrorismo -.			
En la zona de correos no se aplica un protocolo de entrega de paquetería que permita documentar dicha entrega.			

Riesgos Globales			
En zona con amenaza o vulnerabilidad terrorista sin protección y medios de seguridad para controlar el riesgo.			
No aplica un plan de seguridad específico para la edificación.			

ANEXO V: Informes específicos de riesgos evaluados: Representación Gráfica. Mapa de Riesgos