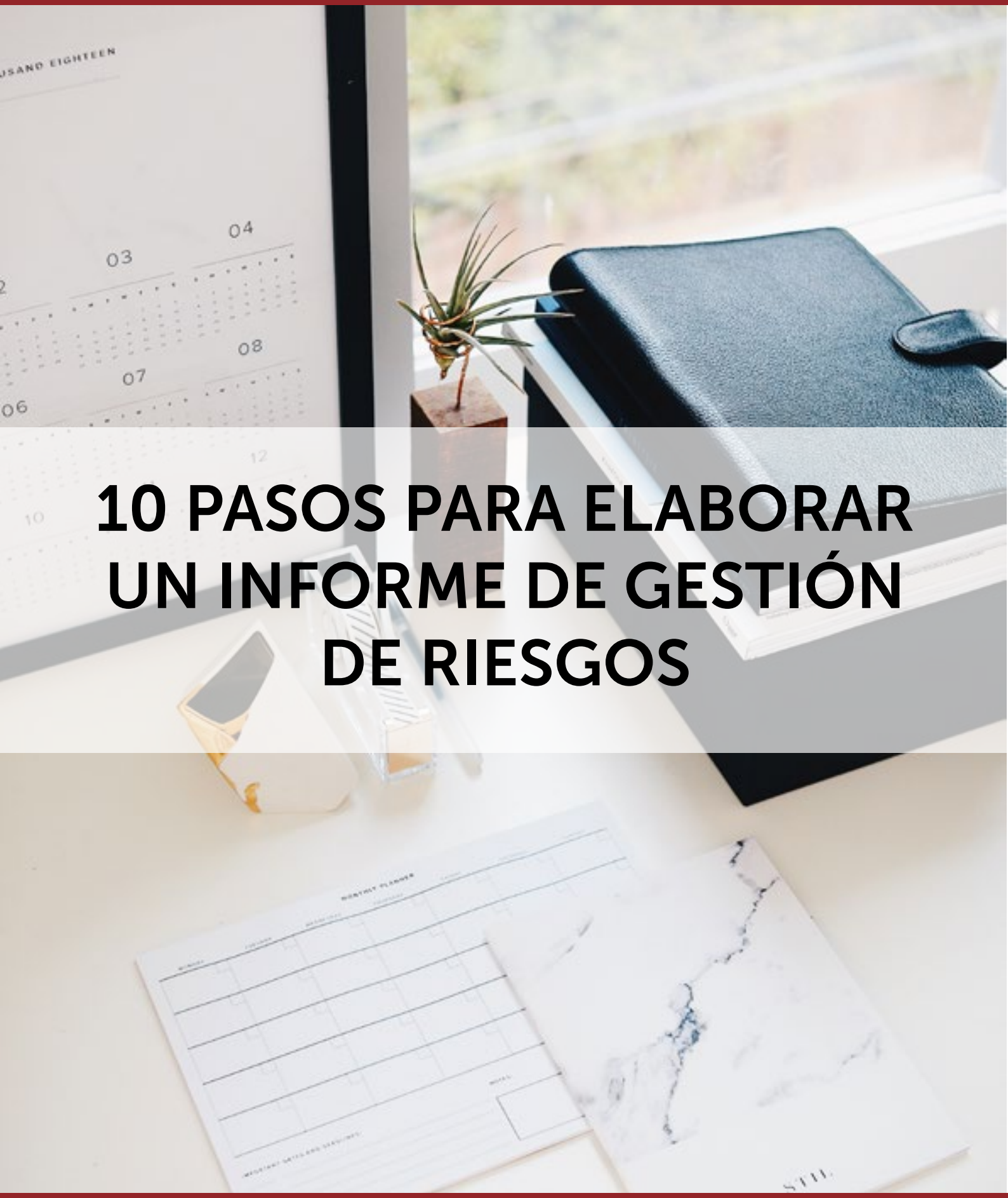
EALDE

Whitepaper



10 PASOS PARA ELABORAR UN INFORME DE GESTIÓN DE RIESGOS

EALDE

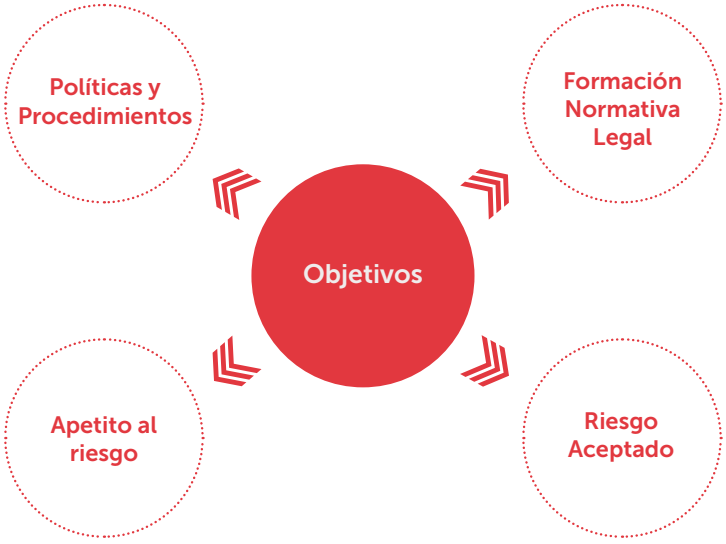
índice

1 LA DESCRIPCIÓN DE LA EMPRESA

La descripción de la empresa comprende el tipo de empresa, su actividad, su función y su ámbito de actuación (nacional o internacional). Se trata de obtener información de la compañía, relativa a su misión, visión, objetivos estratégicos y organigrama.

Esta etapa implica la elaboración de un organigrama de gestión de riesgos óptimo para las características de la empresa y el establecimiento de cuáles son las funciones de cada uno de los miembros de la empresa, sin perder de vista la parte de cultura y gobernanza de la organización. Mucha de esta información es obtenida a partir de los cuadros de mando elaborados.

2 LOS OBJETIVOS



Esta fase comprende los objetivos estratégicos de la empresa y cuáles son los límites a los que ésta puede llegar. La metodología a aplicar puede ser la de las guías de implementación de COSO o normas ISO. Sin embargo, algunas empresas están obligadas a implementar por normativas legales metodologías específicas. Estos objetivos son trasladados a herramientas como el mapa de calor o la matriz de riesgos.

COSO 2013 tiene aplicación desde el 31 de diciembre de 2014 y consta de 17 principios. Las compañías han de observar cuáles de esos principios están siguiendo, cuáles implantar e, incluso, cuáles mejorar. Lo mismo sucede con ISO 31000 y sus 11 principios.

En este apartado entran los manuales y políticas de procedimientos, la normativa que aplica a la empresa y le puede afectar; el apetito al riesgo, tolerancia y capacidad; el riesgo que implican los servicios externalizados; y la elaboración de cuestionarios y políticas para saber cuál es el riesgo aceptado dentro de la compañía.

LA IDENTIFICACIÓN DE RIESGOS

3

Identificación de riesgos » Ficha/Cuestionarios/Listado Riesgos Fraude

En esta etapa se procede a la identificación de los riesgos de la empresa. Éstos pueden ser financieros, legales, estratégicos, operacionales o reputacionales.

En la identificación de riesgos se hace partícipe a toda la organización en la primera línea de defensa, necesaria para poder implementar el sistema de gestión de riesgos. No es suficiente con la involucración de una sola persona o departamento. Se trata de un trabajo en equipo bien distribuido y en el que lo realizado en el día a día va a permitir identificar y trasladar los riesgos a través de fichas, cuestionarios, listados de riesgos, mapas de calor y matrices de riesgos. Debe incorporar un análisis de los riesgos comunes y específicos del sector en el que la empresa desarrolla su actividad.

LA EVALUACIÓN DE RIESGOS

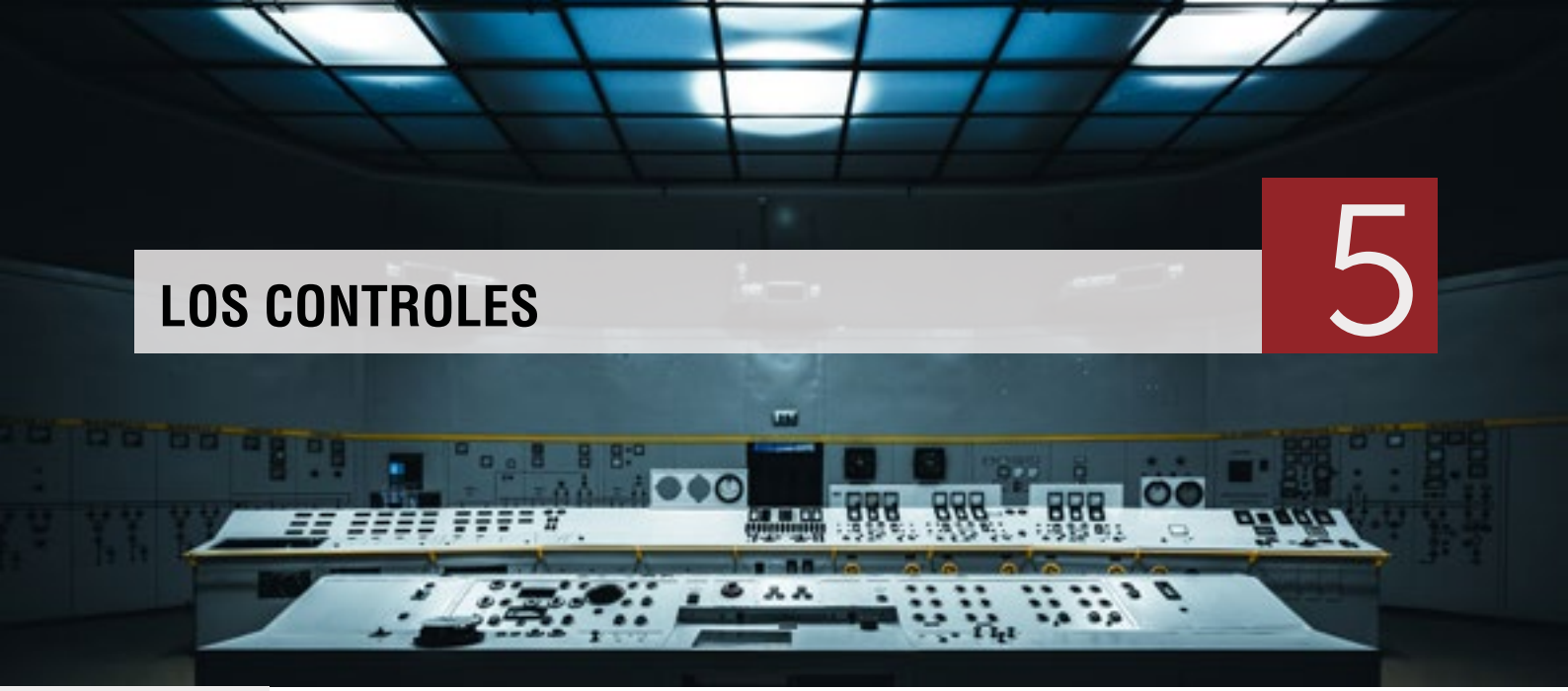
4

La evaluación de riesgos se puede realizar a través de las 31 herramientas de evaluación que proporciona ISO 31010Esta evaluación va a permitir obtener el riesgo inherente de la empresa.

Una vez identificados los riesgos se procede a la evaluación de riegos. Una de las evaluaciones más completas es la de ISO 31010, que recoge 31 técnicas de evaluación, tanto cualitativa como cuantitativa.

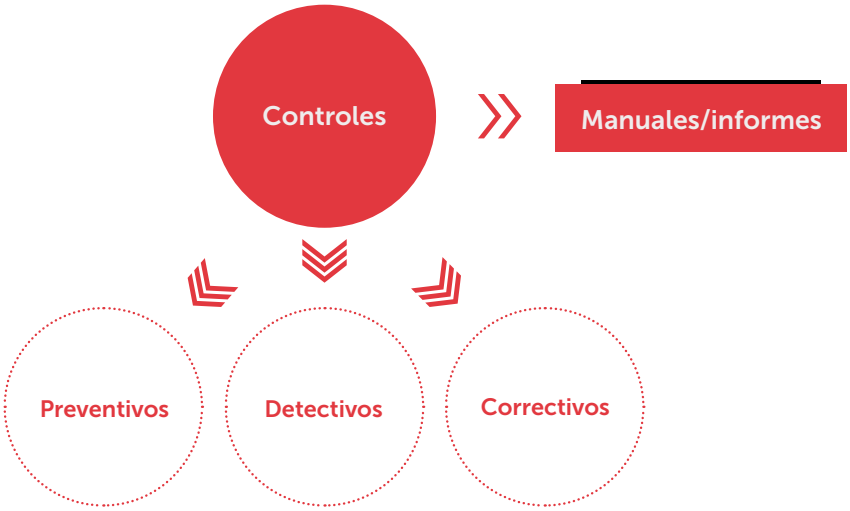
Esta norma permite obtener indicadores y resultados de evaluación. Unos permiten identificar y otros calcular consecuencias, probabilidades. Todas estas herramientas vienen establecidas bajo unos datos de entrada, procesos de cálculo, ventajas e inconvenientes y grado de aplicación.

Con la evaluación se obtiene el riesgo inherente, con lo que la organización puede pasar a centrarse en los riesgos que sobrepasan la zona de confort de la compañía y del apetito al riesgo. Se trata de cuantificar los impactos sucedidos en el pasado, como los que puedan llegar a ocurrir.



LOS CONTROLES

5



Los controles se diferencian en tres categorías: preventivos, detectivos y correctivos. La primera línea de defensa consta de controles de la fase preventiva, en las que se trata de evitar que los riesgos ocurran.

No obstante, siempre hay eventos que no se pueden prevenir y terminan ocurriendo. Estos riesgos se pueden detectar mediante los controles detectivos. Para evitar que estos riesgos vuelvan a suceder, la empresa cuenta con el Plan de Continuidad de Negocio, el Plan de Contingencia y el Plan de Crisis.

Por su parte, los controles correctivos hacen referencia a las correcciones máximas existentes dentro de la organización.

En esta etapa, la figura del compliance contempla el cumplimiento normativo y, por tanto, qué normativa aplica a cada uno de los riesgos identificados dentro de la empresa.

La alta dirección debe considerar qué nuevos controles y medidas se han de adoptar a partir del análisis coste-beneficio. Además, se ha de determinar si los riesgos se tienen que asumir, transferir o minimizar. Para ello, la empresa cuenta con manuales e informes periódicos actualizados y revisados.

EL RIESGO RESIDUAL

6

Riesgo residual » Matriz de riesgo

Con el riesgo inherente y los controles establecidos dentro de la empresa, se obtiene un riesgo residual. Una vez obtenido, este riesgo pasa por el auditor interno de la organización. Consiste en el análisis del riesgo justificado y de los controles eficaces.

El resultado de esta etapa es una matriz de riesgos en la que figura el riesgo inherente y el riesgo residual. Las aportaciones de compliance y auditoría interna proporcionan una matriz de riesgos completa, con una visión amplia del proceso que la empresa está siguiendo.

Esta matriz de riesgos permite tener un conocimiento del riesgo residual amplio, con valor añadido, de modo gráfico y fácil de comprender para el consejo de administración.

LA ESTRATEGIA/TOMA DE DECISIONES

7

La alta dirección y el consejo de administración son los máximos responsables del proceso de gestión de riesgos en las empresas. Después de la obtención del riesgo residual se entra en la fase de estrategia y toma de decisiones. Esta etapa consiste en la ayuda a la alta dirección para la toma de decisiones.

En esta fase, se establece cuál es el coste/beneficio que supone asumir, reducir, eliminar o transferir el riesgo. La toma de decisiones es de este modo más efectiva y está más justificada. En esta parte se recoge toda la normativa, costes de implementación y análisis de costes/beneficios.

Whitepaper

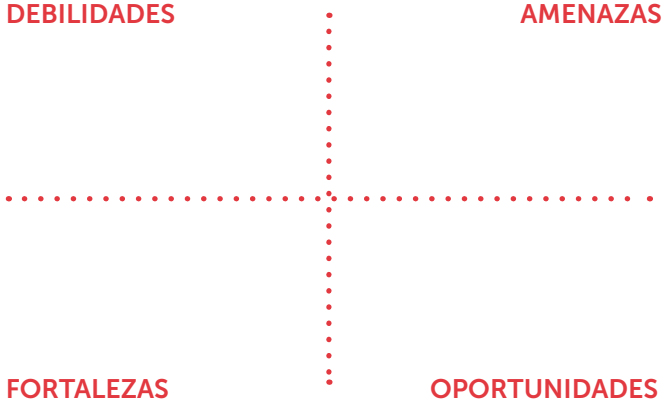
EALDE

LOS PLANES DE ACCIÓN

8

Planes de acción » FODA DAFO » Fortalezas Oportunidades Debilidades Amenazas

ANÁLISIS DAFO



Con el riesgo inherente y los controles establecidos dentro de la empresa, se obtiene un riesgo residual. Una vez obtenido, este riesgo pasa por el auditor interno de la organización. Consiste en el análisis del riesgo justificado y de los controles eficaces.

El resultado de esta etapa es una matriz de riesgos en la que figura el riesgo inherente y el riesgo residual. Las aportaciones de compliance y auditoría interna proporcionan una matriz de riesgos completa, con una visión amplia del proceso que la empresa está siguiendo.

Esta matriz de riesgos permite tener un conocimiento del riesgo residual amplio, con valor añadido, de modo gráfico y fácil de comprender para el consejo de administración.

LA SUPERVISIÓN/AUDITORÍA EXTERNA

9

En este apartado se recoge la información que se va a ofrecer al exterior. Las empresas que cuentan con un proceso interno de implementación de riesgo aportan confianza, con el cumplimiento de normas como ISO o el propio Plan de Continuidad de Negocio. De hecho, hay muchas empresas obligadas a implantar el sistema de gestión de riesgos.

En esta etapa se recoge toda la información obtenida de la organización, para trasladarla en un documento único, el Informe de Gestión de Riesgos.
ge toda la normativa, costes de implementación y análisis de costes/beneficios.

LAS CONCLUSIONES Y RECOMENDACIONES 10

El Informe de Gestión de Riesgos conlleva datos, gráficos, ... e implica también un pronunciamiento dentro de unos límites. El máximo responsable de la implementación del sistema de gestión de riesgos es el Consejo de Administración, pero en base al trabajo realizado por toda la organización.

El trabajo realizado es supervisado por el Área de Gestión de Riesgos o el Gerente de Riesgos. Son estos equipos los que deben comunicar y trasladar todas las apreciaciones o recomendaciones que estimen oportunas al Consejo de Administración.

EALDE

BUSINESS SCHOOL