CAIXA RURAL D'ONDA

Metodología análisis de riesgos

Cumplimiento Normativo

Septiembre 2021

Índice

1 Introducción

1.1 Entorno Normativo

Existe diversa normativa, tanto europea como nacional, que asocia a la Función de Cumplimiento Normativo la obligación de realizar análisis de riesgos periódicos. Dentro de esta hay dos que creemos tienen un impacto significativo en nuestro día a día:

La normativa europea MiFID, es la Directiva que regula los mercados de instrumentos financieros, y es aplicable en la Unión Europea desde noviembre de 2007. En 2014, se publicó la denominada MiFID II que se basaba en la mejora de las reglas ya adoptadas en la anterior normativa. Esta norma entró en vigor el 3 de enero de 2018.

En España, tanto MiFID I como MiFID II, se han traspuesto al ordenamiento jurídico nacional a través de la Ley 47/2007 del 19 de noviembre, el RDL 217/2008 del 15 de febrero, sobre el régimen jurídico de las empresas del servicio de inversión y el RDL 14/2018 por el que se modifica el texto refundido de la Ley del Mercado de Valores aprobado por el RDL 4/2015.

Este entorno normativo, en particular el Reglamento Delegado 565/2017 de la MiFID en su artículo 22.2 establece estos requerimientos para la Función de Cumplimiento Normativo:

> *"Las empresas de servicios de inversión establecerán y mantendrán una función permanente y efectiva de verificación del cumplimiento que actúe con independencia y cumpla los cometidos siguientes:*
>
> *a) supervisar de forma permanente y evaluar con regularidad la adecuación y la eficacia de las medidas, políticas y procedimientos aplicados de conformidad con el apartado 1, párrafo primero, y las medidas adoptadas para corregir cualquier deficiencia en el cumplimiento de las obligaciones de la empresa;*
>
> *b) asesorar y ayudar a las personas pertinentes responsables de la prestación de los servicios y actividades de inversión a efectos del cumplimiento de las obligaciones de la empresa con arreglo a la Directiva 2014/65/UE;*
>
> *c) informar al órgano de dirección, por lo menos anualmente, sobre la instrumentación y la eficacia del entorno de control general de los servicios y actividades de inversión, los riesgos que se han identificado y los informes relativos a la tramitación de reclamaciones, así como las soluciones aplicadas o que deban aplicarse;*
>
> *d) supervisar el funcionamiento del proceso de tramitación de las reclamaciones y considerar las reclamaciones como una fuente de información relevante en el contexto de sus responsabilidades generales de supervisión.*
>
> *Con vistas a cumplir lo dispuesto en las letras a) y b) del presente apartado, la función de verificación del cumplimiento llevará a cabo una evaluación partiendo de la cual establecerá un programa de seguimiento basado en el riesgo que tome en consideración todas los ámbitos de los servicios y actividades de inversión y cualquier servicio auxiliar pertinente de la empresa de servicios de inversión, incluida la información pertinente obtenida en relación con la supervisión de la tramitación de las reclamaciones.*
>
> *El programa de seguimiento deberá establecer las prioridades determinadas por la evaluación del riesgo de cumplimiento asegurando un control exhaustivo del riesgo de cumplimiento*".

En base a estos requerimientos, la ESMA establece en sus directrices para la Función de Cumplimiento Normativo relativa a la implantación de MiFID II que:

> *14. De conformidad con el artículo 22, apartado 2, del Reglamento Delegado MiFID II, la función de cumplimiento, como parte de sus tareas, realizará una evaluación de riesgos para garantizar que los riesgos de cumplimiento se supervisen de forma exhaustiva. La función de cumplimiento establecerá un programa de monitorización basado en el riesgo sobre la base de esta evaluación del riesgo de cumplimiento para determinar sus prioridades y el enfoque de las actividades de monitorización, asesoramiento y asistencia.*
>
> *15. Los resultados de la evaluación del riesgo de cumplimiento deben usarse para establecer el programa de trabajo de la función de cumplimiento y asignar los recursos de las funciones de manera eficiente.*
>
> *La evaluación del riesgo de cumplimiento debe revisarse periódicamente y, cuando sea necesario, actualizarse para garantizar que los objetivos, el enfoque y el alcance de las actividades de supervisión y asesoramiento del cumplimiento sigan siendo válidos.*
>
> *16. Al identificar el nivel de riesgo de cumplimiento que enfrenta la empresa, el segundo párrafo del Artículo 22 (1) del Reglamento Delegado MiFID II requiere que la función de cumplimiento tenga en cuenta todas las áreas de los servicios de inversión, actividades y servicios auxiliares proporcionados por la empresa. Esto debe incluir los tipos de instrumentos financieros negociados y distribuidos, las categorías de clientes de la empresa, los canales de distribución y, cuando corresponda, la organización interna del grupo.*
>
> *17. La evaluación del riesgo de cumplimiento debe considerar las obligaciones aplicables bajo MiFID II, las normas nacionales de implementación y las políticas, procedimientos, sistemas y controles implementados dentro de la empresa en el área de servicios y actividades de inversión. La evaluación también debe considerar los resultados de cualquier actividad de monitorización y de cualquier hallazgo relevante de auditoría interna o externa.*
>
> *18. Los riesgos identificados deben revisarse periódicamente y, cuando sea necesario, también de manera ad-hoc para garantizar que se tengan en cuenta los riesgos emergentes (por ejemplo, como resultado de nuevos campos de negocios, otros cambios relevantes en la estructura de la empresa o en el marco regulatorio aplicable).*

1.2 Riesgo de Cumplimiento Normativo

El riesgo de Cumplimiento Normativo es la posibilidad de incurrir en sanciones legales o administrativas, pérdidas financieras significativas o pérdidas de reputación por incumplimiento de leyes, regulaciones, normas internas y códigos de conducta aplicables, en nuestro caso, a la actividad bancaria.

2 Objeto

Este Manual tiene por objeto definir la Metodología de Análisis de Riesgos que se utilizará en Cumplimiento Normativo de *Caja Rural de Onda* (en adelante *la Entidad*) para la evaluación de los riesgos de cumplimiento y en consecuencia, servir para poder realizar la planificación de trabajos a realizar por dicha Unidad.

3 Alcance

Este manual aplica a la Función de Cumplimiento Normativo de *Caja Rural de Onda*.

4 Departamentos afectados

El contenido de este manual afecta a toda la Entidad.

5 Contenido de la Metodología

Esta *Metodología de Análisis de Riesgos para Cumplimiento Normativo,* incluye la definición de los procedimientos asociados a la identificación, el análisis y la evaluación de los riesgos de cumplimiento para:

a. Identificar los riesgos de cumplimiento que la Entidad pueda razonablemente anticipar, considerando los factores relacionados con la misma y su contexto.

b. Analizar los riesgos de cumplimiento identificados;

c. Evaluar los riesgos de cumplimiento identificados.

d. Poner en marcha las acciones de mejora (Controles) adecuadas para eliminar o mitigar los posibles incumplimientos detectados.

e. Mantener una revisión periódica de los riegos y controles identificados de manera que garantice su adecuación a los requerimientos normativos vigentes.

f. Definir los pasos para identificar posibles incumplimientos y cómo se articularán procedimientos para acordar acciones de mejora que mitiguen o eliminen dichos incumplimientos mediante la implantación de un Plan de Acción.

5.1 Matrices de Riesgo

Para poder identificar los riesgos, así como los controles y/o medidas mitigatorias, esta Metodología utilizará las *Matrices de Riesgo (también llamadas Mapas de Riesgo)*. Las matrices de Riesgos será la herramienta utilizada por esta metodología para identificar los riesgos a los que está expuesta la Entidad dentro del ámbito de actuación de Cumplimiento Normativo.

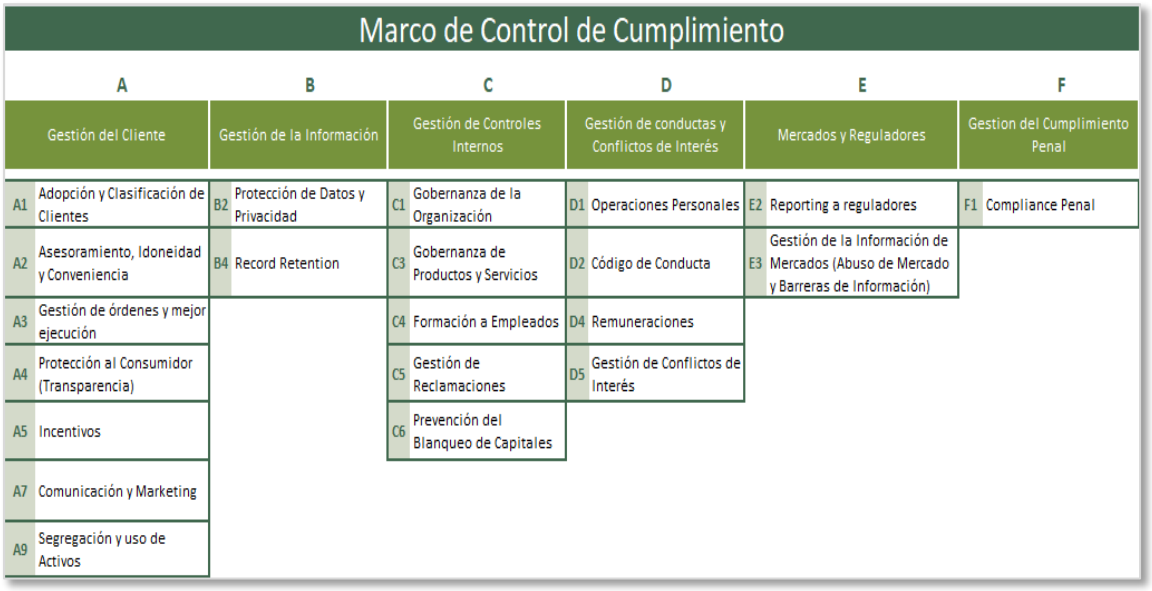
Para poder definir unas *Matrices de Riesgo* adecuadas, lo primero que debemos tener es un conocimiento total de las líneas de negocio que nuestra Entidad aborda en su actividad, incluyendo el personal y la infraestructura utilizada para dar soporte a dicho negocio.

Cumplimiento Normativo debe estar constantemente informado de los cambios que puedan surgir en las líneas de negocio y en la estructura de la Entidad. Esto ayudará a garantizar que las matrices de riesgo reflejen la situación de la Entidad en todo momento.

En este sentido, es importante identificar una serie de factores que ayudarán en esta labor, a saber:

- El objeto social y productos o servicios que la empresa comercializa
- El tipo de infraestructura que tiene la empresa
- La zona geográfica de influencia en la actividad de la empresa
- La distribución interna y externa de las partes que integran la empresa
- Organización de los mandos de la empresa y demás órganos involucrados en la toma de decisiones
- Delimitación de contenido y actuación del Programa de Compliance

Nuestro Manual de Cumplimiento Normativo identifica el *ámbito de actuación* de la Unidad de Cumplimiento Normativo. Este ámbito de actuación se ha dividido en Áreas de Cumplimiento, que a su vez se componen de Secciones de Cumplimiento, que se muestran en el cuadro adjunto:



Marco de Control de Cumplimiento					
A	B	C	D	E	F
Gestión del Cliente	Gestión de la Información	Gestión de Controles Internos	Gestión de conductas y Conflictos de Interés	Mercados y Reguladores	Gestion del Cumplimiento Penal
A1 Adopción y Clasificación de Clientes	B2 Protección de Datos y Privacidad	C1 Gobernanza de la Organización	D1 Operaciones Personales	E2 Reporting a reguladores	F1 Compliance Penal
A2 Asesoramiento, Idoneidad y Conveniencia	B4 Record Retention	C3 Gobernanza de Productos y Servicios	D2 Código de Conducta	E3 Gestión de la Información de Mercados (Abuso de Mercado y Barreras de Información)	
A3 Gestión de órdenes y mejor ejecución		C4 Formación a Empleados	D4 Remuneraciones		
A4 Protección al Consumidor (Transparencia)		C5 Gestión de Reclamaciones	D5 Gestión de Conflictos de Interés		
A5 Incentivos		C6 Prevención del Blanqueo de Capitales			
A7 Comunicación y Marketing					
A9 Segregación y uso de Activos					

Para poder gestionar los riesgos y controles existentes en cada una de las Áreas/Secciones de Cumplimiento se han implantado una *Matrices de Riesgo* asociada a cada Sección.

Estas *Matrices de Riesgo* nos permiten tener una visión completa de los riesgos a los que estamos expuestos por nuestro negocio, la identificación de las medidas mitigadoras implantadas, y en caso contrario, la identificación de los planes de acción a poner en marcha para implantarlas y así subsanar las deficiencias encontradas. Esto nos permitirá disponer del entorno de control más robusto posible.

La configuración de las *Matrices de Riesgo* deben revisarse al menos una vez al año o cuando se produzcan cambios significativos en la normativa aplicable y/o procesos internos asociados (cambios en sistemas, procedimientos, etc.). También si como resultado de una revisión de una sección se detecten mejoras y/o la necesidad de añadir elementos nuevos a la Matriz (Riesgos, Controles o Datos).

Estos mapas, contendrán una relación de cualquier tipo de infracción o incumplimiento en el que puede incurrir nuestra Entidad, puestos en relación con las actividades o sectores internos en los que dichos riesgos se podrían materializar con la probabilidad e impacto de los mismos. Adicionalmente se incluirán los posibles impactos para la Entidad que pueden producirse en caso de que se identifiquen incumplimientos.

Asimismo, incluirá una valoración de la adecuación del diseño y eficacia de los controles existentes en la Entidad.

En el caso de identificación de deficiencias en determinados controles, la Entidad tomará las medidas oportunas para remediarlas, implantando planes de acción que mitiguen los riesgos asociados a dichos controles.

La identificación, análisis y evaluación de los riesgos penales se realizará en la herramienta interna Motor de Cumplimiento (*MC360* de ahora en adelante), utilizando una metodología de análisis propia, que se describe a continuación.

5.2 Conceptos a tener en cuenta en esta metodología

A continuación se incluye una descripción de ciertos conceptos utilizados por esta metodología:

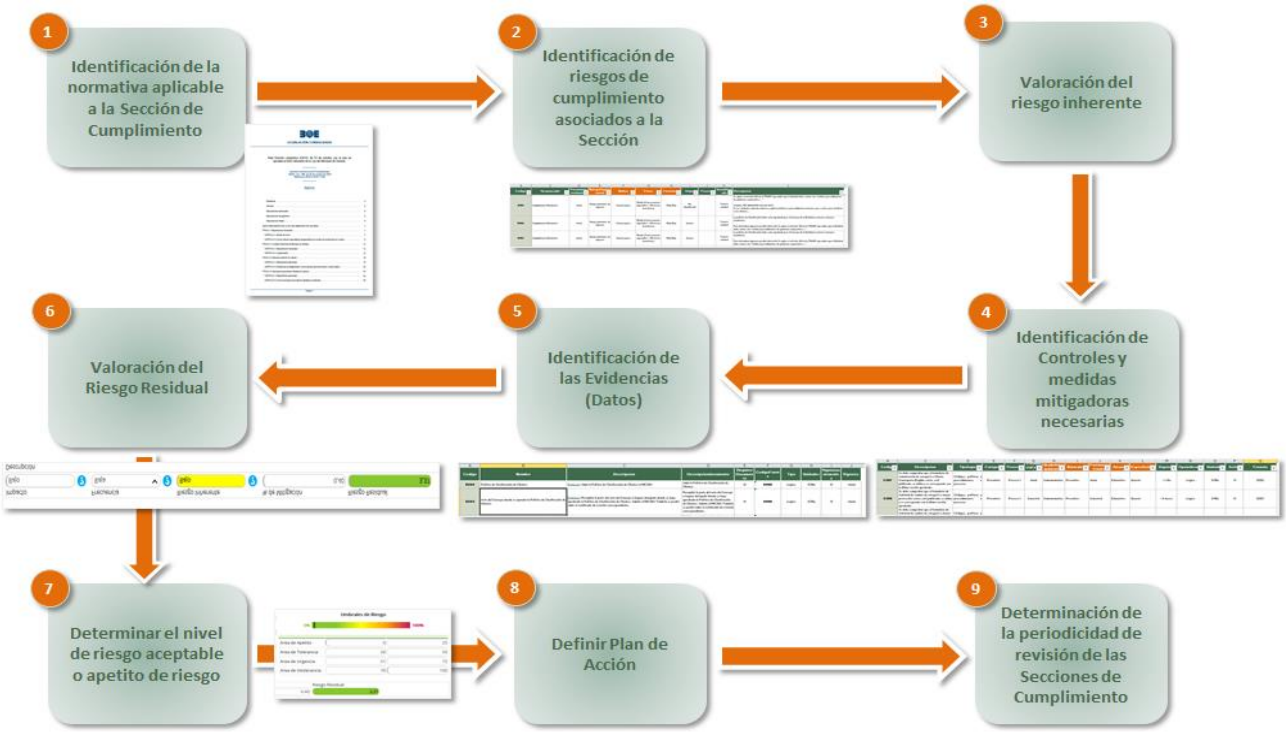
Riesgo Reputacional	Banco de España define este tipo de Riesgo como el derivado de actuaciones de la entidad que posibiliten una publicidad negativa relacionada con sus prácticas y relaciones de negocios, que pueda causar una pérdida de confianza en la institución, y por esta vía afectar a su solvencia. También pueden ser consecuencia de una actuación atribuida a la entidad. Esto puede llegar a afectar no sólo a la solvencia sino también a otros aspectos como pérdida de clientes, sanciones, dificultad de acceso a financiación, etc. Como consecuencia de esto, la Entidad podría poner en riesgo la continuidad de su negocio.
Riesgo Inherente	Es el riesgo que resulta con anterioridad al tratamiento o intento de control del mismo; el que se ha identificado con carácter previo a la implantación de cualquier tipo de medida de mitigación o control diseñado para su prevención
Riesgo Residual	Se trata del nivel de riesgo que permanece activo en nuestra Entidad, habiendo aplicado los controles diseñados para su prevención o inhibición. Esto es, el riesgo remanente tras efectuar su análisis.
Riesgo de Sanción	En caso de incumplimiento de la normativa existe el riesgo de sanción por parte de las autoridades competentes. En este caso, dependiendo de la norma incumplida, se refleja el potencial impacto.
Pérdida Financiera Material	Es la posible sanción aplicable al realizar un incumplimiento de una Norma. El importe puede variar en función de si se considere que el incumplimiento ha sido reiterado o puntual. Se traduce en importe monetario de la sanción.
% Mitigación	Cuando se identifica un Riesgo, la Entidad diseña una serie de controles o medidas mitigantes, cuyo objetivo es reducir o eliminar dicho riesgo. El % de mitigación es, en base porcentual, cómo los controles o medidas han mitigado el riesgo. Un 100% de mitigación indicará que el riesgo ha sido mitigado en su totalidad.

6 Proceso de análisis de Riesgos en Cumplimiento Normativo (Matrices de Riesgo)

Nuestra Metodología de Gestión de Riesgos se apoyará en la Herramienta *MC360*, para parametrizar y gestionar las matrices de Riesgo. Esta herramienta además será utilizada para evaluar el nivel de cumplimiento de la Entidad respecto de las Secciones de Cumplimiento identificadas y parametrizadas en ella. Esta herramienta por tanto nos ayudará a calcular el nivel de riesgo existente (inherente y residual), a identificar incumplimientos y a crear y gestionar planes de acción para mitigar y/o eliminar los incumplimientos detectados.

Los resultados de las revisiones realizadas nos ayudarán a identificar posibles mejoras en las matrices de riesgos existentes, así como en su diseño (riegos, controles y evidencias).

El proceso de creación y evaluación de las *Matrices de Riesgo* en nuestra Metodología se compone de los siguientes pasos:



Las matrices de Riesgo que utilizaremos dispondrán de 4 apartados de información principales:

1. Sección de Cumplimiento.
2. Riesgos
3. Controles o medidas mitigatorias
4. Datos o evidencias

En los apartados que mostramos a continuación, se explican en detalle las acciones a realizar en cada uno de los pasos arriba mostrados.

6.1 Matriz de Riesgos: Apartado de Sección de Cumplimiento

Este apartado de la matriz de riesgos contendrá la parametrización de la Sección de Cumplimiento a la que aplique dicha matriz. Una vez este apartado se haya completado, estará listo para ser cargado en el Motor de Cumplimiento, nuestra herramienta de soporte a esta metodología y que será la encargada de realizar los cálculos necesarios para determinar el nivel de riesgo que la Entidad está asumiendo en la Sección de Cumplimiento analizada.

6.1.1 Información necesaria para la Matriz de Riesgos

En primer lugar deberemos analizar qué normativa nos aplica, y por tanto qué requerimientos debemos cumplir para determinar los Riesgos y Controles asociados. Para ello será necesario identificar las líneas de negocio asociadas al ámbito de actuación de Cumplimiento Normativo y analizar qué requerimientos regulatorios existen asociadas a dichas líneas de negocio.

En este apartado habrá que poner especial atención para identificar si además de la normativa a nivel de Entidad, existen requerimientos específicos a cumplir por parte de las Unidades de Cumplimiento Normativo.

En la matriz de Riesgo, en el *apartado de Sección*, deberá recopilarse la siguiente información:

1	***Código de Sección***
	Código de sección único que se corresponde con el asignado en el Marco de Actuación de la Unidad de Cumplimiento Normativo.
2	***Descripción***
	Definición del alcance de la Sección. Coincide con la descripción incluida en este Manual.
3	***Responsable***
	Se asignará un responsable de coordinación a cada Sección. Estos responsables estarán parametrizados en el Motor de Cumplimiento.
4	***Alcance***
	El alcance determina si la sección aplica a toda la Entidad o a una actividad concreta.
5	***Frecuencia evaluación***
	Determinará la frecuencia de evaluación normal de la sección. Esta se verá afectada por el resultado de las revisiones realizadas (ver apartado 5.8 de este documento).
6	***Peso en el indicador global***
	Establece el peso de la norma dentro del ámbito de actuación de Cumplimiento Normativo. Los posibles valores irán desde 1 (poco peso) hasta 10 (máximo peso). Se recomienda como mínimo un peso de 5 puntos.

MC360 calculará el nivel de cumplimiento de la Sección evaluada, considerando para ello el nivel de cumplimiento de los elementos relacionados con ella (riesgos y controles asociados):

El sistema realizará un análisis del nivel de cumplimiento de cada uno de los riesgos. Una vez obtenido este resultado, el sistema evaluará el umbral de riesgo del conjunto de los riesgos asociados a la Sección, considerando para ello, la ponderación de cada Riesgo (los riesgos pueden tener una ponderación de 1 a 10, siendo 1 menor valor y 10 mayor valor).

Como resultado de este análisis el Sistema nos suministrará la siguiente información:

- Riesgo de Sanción. Se realizará una media ponderada de los riesgos de sanción identificados en los riesgos asociados a la Sección evaluada, considerando, como hemos indicado, el peso de cada riesgo en dicha Sección.
- Pérdida financiera material. De igual forma que en el riesgo de sanción, la perdida material financiera de la Sección evaluada, será el resultado de calcular la media ponderada de las posibles pérdidas financieras identificadas en los riesgos asociados considerando el peso de cada riesgo en dicha Sección.
- Riesgo Reputacional. Resultado de aplicar el mismo cálculo explicado anteriormente, pero aplicado al riesgo reputacional identificado para los riesgos asociados a la Sección evaluada.
- Impacto. Se calculará con el resultado de los campos anteriormente mencionados, y será el máximo rating obtenido en los tres parámetros evaluados (Impacto = máximo rating de los criterios empleados (Tipo de sanción, Pérdida material financiera y Riesgo reputacional)).
- Frecuencia. Se calculará la media ponderada de la frecuencia identificada a los riesgos asociados a la Sección.
- Riesgo Inherente. El riesgo inherente se mostrará tanto en su valor cuantitativo (numérico, en porcentaje) como cualitativo (descripción) y resultará de multiplicar el impacto por la frecuencia. Los posibles valores serán:

Categoría	Valor Riesgo Inherente		Definición
	Número	%	
Extremo	15 a 25	60% a 100%	Este riesgo debería ser eliminado, traspasado, compartido o reducido.
Alto	9 y 14	36% a 59%	Este riesgo debería ser traspasado, compartido o mitigado
Moderado	6 y 8	24% a 35%	Este riesgo normalmente será reducido
Bajo	4 y 5	16% a 23%	El comité de Dirección tomará una decisión sobre si el riesgo debe ser asumido o reducido-
Muy bajo	1 y 3	1% a 15%	Este riesgo puede ser asumido

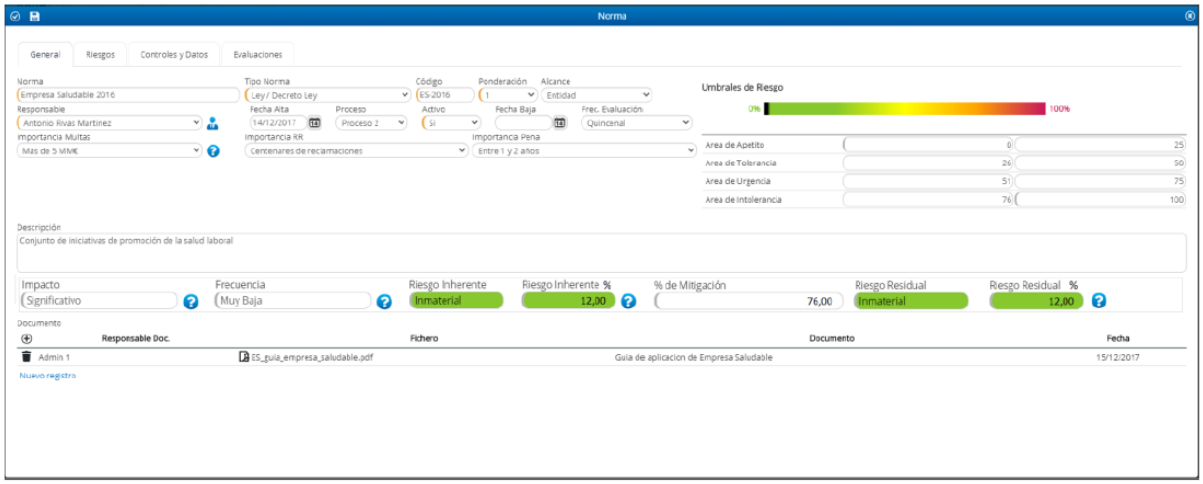
- Riesgo Residual. Se mostrará también en su valor cuantitativo (numérico en porcentaje) como cualitativo (descripción). Los posibles valores serán:

Categoría	Número	Valor Riesgo Residual %
Extremo	15 a 25	60% a 100%
Alto	9 y 14	36% a 59%
Moderado	6 y 8	24% a 35%
Bajo	4 y 5	16% a 23%
Muy bajo	1 y 3	1% a 15%

- Ubicación en Umbral de Riesgo. El resultado obtenido en el Riesgo Residual, nos ubicará la norma en una de los cuatro umbrales de Riesgo identificados en esta Metodología, y

nos determinará la periodicidad con la que la Sección de Cumplimiento habrá de ser revisada (*ver apartado 5.8 de este documento*).

La información sobre el estado de la Sección, una vez evaluada, será mostrada en el Motor de Cumplimiento, en la siguiente pantalla:



De esta manera en una sola pantalla tendremos toda la información actualizada de la Sección que estemos consultando.

6.2 Matriz de Riesgos: Apartado de Riesgos de Cumplimiento

Cuando se definen y/o revisan las Áreas/Secciones de Cumplimiento incluidas en el Marco de Actuación, se deben identificar los posibles riesgos, que estarán, en gran medida, asociados a la normativa interna o externa aplicable a las mismas.

La tarea de identificación de los riesgos es una actividad dinámica en constante actualización, nunca una imagen fija de la empresa. De nada servirá tener un mapa de riesgos que se haya elaborado con demasiada antigüedad si los riesgos que se encuentran relacionados en el mismo no se han actualizado desde entonces.

Es necesario contar con toda la información posible de la empresa, para lo que se debe tener un contacto constante con todo el personal que la compone.

De acuerdo con lo anterior, es posible enumerar diferentes categorías en las que clasificar los escenarios en los que suelen elementos de riesgo. Estos escenarios pueden ser:

- Escenarios ligados a la actividad de la empresa
- Escenarios ligados al propio servicio o producto
- Escenarios ligados a las zonas geográficas de influencia en la actividad de la empresa
- Escenarios ligados a la conducta interna

Como hemos comentado anteriormente, este proceso será dinámico, y nos permitirá identificar y evaluar los riesgos existentes asociados a las normas de aplicación a la Sección de Cumplimiento que estemos analizando. Estos riesgos serán evaluados en relación a unos niveles preestablecidos de tolerancia (que serán mencionados más adelante).

6.2.1 Información necesaria para la Matriz de Riesgos

Para poder evaluar adecuadamente los riesgos identificados, necesitaremos, por cada riesgo, una serie de datos (algunos estáticos y otros variables). En el caso de los datos variables, se han definido una serie de valores, que tendrán impacto en el cálculo posterior del riesgo inherente.

En la matriz de Riesgo, en el *apartado de Riesgos*, deberá recopilarse la siguiente información:

1 *Código de riesgo*

Identificador del Riesgo. Será un código compuesto de una "**R**" más un número secuencial.

2 *Riesgo*

Nombre o Título del Riesgo.

3 *Descripción del Riesgo*

Descripción del riesgo, incluyendo normativa asociada.

4 *Riesgo Reputacional*

Se han definido 5 posibles valores:

Riesgo Reputacional	*Rating*	*Descripción*
Quejas puntuales sin impacto	***5***	*Se pueden producir algunas quejas, pero no generan impacto en la Entidad.*
Reclamaciones puntuales con impacto	***4***	*Pocas reclamaciones pero con posible impacto*
Reclamaciones numerosas con mucho impacto y aparición puntual RRSS y MC	***3***	*El número de reclamaciones es elevado y puede aparecer en medios y prensa.*
Aparición con difusión significativa RRSS y MC	***2***	*Independientemente del número de reclamaciones, la difusión en medios es significativa.*
Aparición con difusión masiva RRSS y MC	***1***	*Gran aparición en medios y prensa. Impacto reputacional elevado.*

5 *Riesgo de Sanción*

No cumplir con lo establecido nos puede generar algún tipo de sanción, según lo indicado por la normativa. Se han definido los siguientes valores que deberán asignarse a cada Riesgo de la Matriz:

Posible sanción aplicable	*Rating*	*Descripción*
NO APLICA SANCIÓN	***5***	*El incumplimiento no genera ninguna sanción*
SANCIÓN LEVE	***4***	*La sanción que puede acarrear el riesgo es leve*
SANCIÓN MEDIA	***3***	*La sanción se considera como nivel medio*
SANCIÓN GRAVE	***2***	*En este caso la sanción puede acarrear consecuencias graves*
SANCIÓN MUY GRAVE	***1***	*Consecuencias muy graves para la Entidad.*

6 *Perdida Financiera Material*

Nos marcará el posible impacto de perdida financiera. 5 posibles opciones:

Impacto	*Rating*	*Descripción*
MUY BAJO	***5***	*Poca afectación, < 1% de los beneficios*
BAJO	***4***	*Inconveniencias no significativas, < 5% de los beneficios*
MEDIO	***3***	*Consecuencias superables < 10% de los beneficios*
ALTO	***2***	*Consecuencias superables sin dificultades, < 20% de los beneficios*
MUY ALTO	***1***	*Consecuencias difícilmente superables, > 20% de los beneficios*

7 *Área afectada*

Área afectada por el riesgo. Puede ser toda la Entidad o un área concreta de la misma

8 *Impacto*

Una vez se ha identificado:

- El riesgo reputacional, asociado
- El tipo de sanción, que podría generarse si el riesgo se lleva a efecto,
- Se ha identificado qué tipo de pérdida material financiera podría materializarse,

Se procede a analizar el posible impacto. El impacto se refiere al conjunto de consecuencias que tendría el evento dañoso en caso de que se acabase materializando, es decir, es la pérdida estimada por la materialización del evento de riesgo, en promedio o severidad.

En el análisis, conviene otorgar una escala valorativa del mismo. En nuestro caso, se ha establecido una escala de 1 (despreciable) a 5 (máximo). La evaluación del impacto vendrá dada por el mayor valor (más crítico) que se tome en los tres atributos (sanción, reputacional y pérdida financiera) y se asignará como valor de impacto en la herramienta de forma automática.

Es decir, el ***Impacto = máximo rating de los criterios empleados***

Impacto	*Rating*	*Tipo de Sanción*	*Riesgo Reputacional*	*Perdida Material Financiera*
Máximo	**5**	Muy grave	Aparición con difusión masiva Redes Sociales (RRSS) y Medios de Comunicación (MC)	Muy Alto (consecuencias superables difíciles, > 20% de los beneficios)
Alto	**4**	Grave	Aparición con difusión masiva RRSS y MC	Impacto Alto (consecuencias superables sin dificultades, < 20% de los beneficios)
Medio	**3**	Media	Reclamaciones numerosas con mucho impacto y aparición puntual RRSS y MC	los beneficios) Medio (Consecuencias superables < 10% de los beneficios)
Bajo	**2**	Baja	Reclamaciones puntuales con impacto	Bajo (Inconveniencias no significativas, < 5% de los beneficios)
Despreciable	**1**	No aplica o muy leve	Quejas puntuales sin impacto	Muy bajo (poca afectación, < 1% de los beneficios)

9 *Frecuencia o Probabilidad*

Se trata de la frecuencia con la que teóricamente se podría llegar a producir el riesgo al no haber controles que la mitiguen. Así, es importante resaltar el hecho de que la probabilidad se mide en términos puramente teóricos, sin tener en cuenta nada más que la propia contextualización de nuestra Entidad realizada en un primer momento y el evento dañoso en sí mismo, pues cuantificar dicho parámetro es un paso previo a la medición del riesgo residual que se calculará en un momento posterior.

Al igual que el impacto, es necesario otorgar una escala valorativa que mida la probabilidad en unos valores cuantificables. En nuestro caso se utilizará una escala de 1 a 5 según se indica en la tabla adjunta:

Frecuencia	*Rating*	*Descripción*
Muy Alta	**5**	Muy elevada (se han dado multitud de circunstancias irregulares en el pasado. Es una actividad realizada diariamente que puede ser realizada por cualquier miembro de la organización)
Alta	**4**	Elevada (Se han dado circunstancias irregulares en el pasado y es una actividad que se realiza semanalmente por Directivos).
Media	**3**	Posible (Se ha dado alguna circunstancia ocasional irregular en el pasado y es una actividad realizada mensualmente por un número amplio de empleados)
Baja	**2**	Improbable (No se han dado circunstancias irregulares hasta ahora. La actividad se realiza anualmente y en todo caso por un número reducido de empleados
Muy Baja	**1**	Muy improbable de que ocurra esta circunstancia en la Entidad.

6.2.2 Cálculo del Riesgo inherente

Se trata del riesgo intrínseco a la propia actividad de la que se desprende. También se puede definir como el riesgo que resulta con anterioridad al tratamiento o intento de control del mismo; el que se ha identificado con carácter previo a la implantación de cualquier tipo de medida de mitigación o control diseñado para su prevención.

Riesgo Inherente = Frecuencia o probabilidad de que ocurra* x Impacto estimado*

* Frecuencia: probabilidad de ocurrencia de evento no deseado sin considerar las acciones y controles mitigantes.
** Impacto: es el impacto de un evento, sin considerar las acciones y controles mitigantes.

En nuestra metodología se ha definido como un valor máximo de 25 puntos (máximo impacto y máxima frecuencia (5x5, según los valores explicados anteriormente) y un mínimo de 1 punto (mínimo impacto y mínima frecuencia: 1x1, según los valores explicados anteriormente).

Los posibles valores del Riesgo inherente, serían:

Categoría	Escala Valor Riesgo	Definición
Muy Alto	Entre 15 a 25	Este riesgo debería ser eliminado, traspasado o mitigado.
Alto	Entre 9 y 14	Este riesgo debería ser traspasado o mitigado
Moderado	Entre 6 y 8	Este riesgo debería ser mitigado
Bajo	Entre 4 y 5	Este riesgo debería ser mitigado o asumido
Muy bajo	Entre 1 y 3	Este riesgo debería ser asumido

Definidos los riesgos inherentes se deben identificar los controles mitigantes y de ahí resultará el riesgo residual que trataremos más adelante.

6.2.3 Parametrizando MC360: Asociación de los riesgos a la Sección

En la Matriz de Riesgos procederemos a asociar los riesgos a la Sección, de manera que nos permita parametrizar el MC360. Para ello, dentro de la matriz de Riesgo, en una tabla específica, relacionaremos los Riesgos y las medidas y controles relacionados.

- Ponderación: La Ponderación será la importancia que tenga ese riesgo dentro de la Sección. Los posibles valores irán de 1 (menor importancia) a 10 (mayor importancia).

Un ejemplo de la tabla sería:

CodNorma	CodRiesgo	Ponderacion
A1	R165	5
A1	R166	5

6.3 Identificación de Controles y medidas mitigadoras necesarias

Una vez identificadas los riesgos de las Áreas/Secciones y la normativa aplicable, hay que identificar e inventariar las medidas mitigadoras y controles existentes que cubran dichos riesgos anteriormente detectados y aquellos otros que sea necesario implantar adicionalmente para que el riesgo quede adecuadamente cubierto.

Los controles serán pues aquellas medidas preventivas que se van a encargar de atenuar y evitar la consecución del evento dañoso que se pretende evitar. Estas medidas pueden llevarse a cabo a través de políticas y procedimientos que contribuyen a que se lleven a cabo las instrucciones de la dirección orientadas a mitigar o eliminar los riesgos con impacto potencial.

Por su parte, las actividades de control se ejecutarán en todos los niveles de la Entidad y en las diferentes etapas de los procesos de negocio (por su puesto incluyendo el entorno tecnológico que de soporte a dichos procesos).

Existen diferentes tipos de controles según su naturaleza, aunque en términos resumidos podemos hablar de dos grandes grupos de controles:

a. **Controles preventivos**: están diseñados con el objetivo de eliminar las causas del riesgo o evento dañoso para prevenir que acabe materializándose.
b. **Controles detectivos**: están diseñados para el manejo del evento dañoso una vez materializado el riesgo, no para prevenir la materialización del mismo, de modo que sus efectos se despliegan en un momento posterior a su materialización al objeto de corregir dicha materialización desde el primer momento.

Una vez relacionados los escenarios de riesgo inherente junto con los controles diseñados para la evitación, inhibición o reducción del impacto de los mismos, habremos evaluado cada escenario de riesgo y se podrá establecer una nueva escala valorativa del mismo. Esto es especialmente relevante para determinar cuáles de los riesgos residuales resultantes de esta valoración son asumibles por la empresa y cuáles se deben suprimir completamente.

6.3.1 Información necesaria para la Matriz de Riesgos

En la matriz de Riesgo, en el *apartado de Controles*, comenzaremos a identificar los controles o medidas mitigatorias necesarias o que hayamos identificado. Para cada uno de ellos se deberá recopilar una serie de información y/o evaluar su situación. Esta información será muy importante para poder evaluar posteriormente la fortaleza de dichos riesgos.

1	***Código de Control***
	Código único asignado al Control. Comenzará con una "**C**" y un número secuencial.
2	***Nombre del Control***
	Nombre corto del control...
3	***Descripción del Control***
	Descripción del Control.
4	***Tipología***
	Varias opciones:

Frecuencia	*Comentarios*
ACTUACIONES DE CONTROL	Corresponde a aquellos controles que en sí mismo son controles sobre el funcionamiento de algún control ya existente, proceso o procedimiento. Se obtienen resultados que nos permitirán determinar el funcionamiento adecuado o no de dicho control, proceso o procedimiento.

AUDITORÍAS DE TERCEROS	Cuando el control se realiza sobre una auditoría realizada por departamentos de auditoría externa a la Entidad
AUDITORÍAS INTERNAS	Cuando el control se realiza sobre una auditoría realizada por departamentos de auditoría externa a la Entidad
CÓDIGOS POLÍTICAS Y PROCEDIMIENTOS O PROCESOS	Son controles sobre la existencia y contenido, de políticas y procedimientos de la Entidad.
CONTROLES INFORMÁTICOS	Controles resultado de un proceso automático concreto
FORMACIÓN	Controles sobre formación
ORGANIZATIVOS	Controles sobre aspectos organizativos de la Entidad (aprobación de documentos, actas, etc…)

5 *Grado de Automatización*

De igual forma que en otros parámetros, dependiendo del grado de automatización se le asignarán valores que van del 1 al 5. Varias posibilidades:

Grado	*Rating*	*Descripción*
AUTOMÁTICO	***5***	*Control embebido en los sistemas que de manera automática establece y fuerza a utilizar una serie de reglas predefinidas*
SEMIAUTOMÁTICO	***3***	*Combinación de trabajo manual más el apoyo de alguna herramienta informática*
MANUAL	***1***	*El control se realiza de manera manual. No hay intervención de elementos tecnológicos*
NO APLICA	***0***	*Cuando un control no depende de procesos manuales o no, por ejemplo la existencia o no de una política.*

6 *Naturaleza*

El algoritmo de cálculo de la fortaleza del control permite dos posibles valores, con una puntación de 1 a 5:

Grado	*Rating*	*Descripción*
PREVENTIVO	***5***	*Un control interno que se usa para prevenir eventos no deseados, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso o producto final, de acuerdo a la organización. Recibe la máxima puntuación*
DETECTIVO	***1***	*Un control interno que se usa para detectar eventos no deseados, errores u otras ocurrencias que pudieran tener un efecto material negativo sobre un proceso ya finalizado. Recibe la menor puntuación*

7 *Frecuencia del control*

Periodicidad con que se ejecuta el control. Se le asignará un rating distinto en función de la periodicidad con la que el control sea ejecutado:

Frecuencia	*Rating*	*Comentarios*
DIARIA	**5**	El algoritmo para calcular la fortaleza del control le otorga la máxima calificación.
MENSUAL	**4**	No es necesario realizar el control diariamente y por tanto tiene algo menos de fortaleza
TRIMESTRAL	**3**	El control se realiza 4 veces al año, y su fortaleza será media debido a esta frecuencia
SEMESTRAL	**2**	Control realizado dos veces al año, fortaleza débil.
ANUAL	**1**	El control se realiza una vez al año, no se dedica una monitorización periódica y por tanto se le aplica menor puntuación
NO APLICA	**0**	Cuando el control no depende de su frecuencia

8 *Alcance*

Tres posibles valores, que recibirán puntuación de 1 a 5 puntos:

Grado	*Rating*	*Descripción*

EXHAUSTIVO	***5***	*Se revisa el 100% de los casos*
MUESTRAL	***1***	*Se selecciona una muestra representativa en el control, no el 100% de los casos*
NO APLICA	***0***	*Se selecciona este valor cuando el alcance no afecte a la efectividad del control. No recibe puntos*

9	***Especificidad***
	Si el trabajo realizado para este control es general (vale para varios controles, recibe 5 puntos) o específico del control (recibe 1 punto).
10	***Criticidad en la solución***
	Cuanto tiempo tenemos para resolver un incumplimiento en ese control. Las opciones son: *<1 día*, <1 semana, <1 mes, < 6 meses o <1 año.
11	***Tipo de indicador asociado al control***
	Marca en qué formato va a recibir el control, en el MC360, la información asociada a su funcionamiento. Podrá ser *numérico* (se basa en un número resultado del control) o l*ógico* (si/no, es decir, el control se realiza y cómo se realiza).
12	***Fórmula***
	Indicará como el MC360 va a calcular el cumplimiento del Control. Esta fórmula indica los datos (evidencias) asociados al control. Si el comportamiento de éstas es el correcto, el cumplimiento del control será adecuado, sino, se podrá producir un incumplimiento en el control.

6.3.2 Calculando la fortaleza del control

En este apartado se evaluará la efectividad o fortaleza del Control. Esta metodología establece 5 posibles niveles de fortaleza en función del valor obtenido por el control (Rating) que podrá ir de 1 (peor nivel de fortaleza) a 25 (máximo nivel de fortaleza) más el resultado de los puntos 5 a 9 de la tabla anterior.

Según el control se ubique en uno de los 5 niveles posibles, se le asignará un porcentaje máximo de mitigación de los riesgos asociados, que irá desde el 5% (peor rating) a 80% (mejor rating).

Rating obtenido	Fortaleza del control	% Mitigación
De 1 a 5	No consta control apreciable. La fortaleza prácticamente no existe.	*5*
De 6 a 10	Muy débil. Necesita mejoras considerables	*20*
De 11 a 15	Débil. Necesita mejorar	*40*
De 16 a 20	Fuerte, pero todavía mejorable	*60*
De 21 a 25	Muy Fuerte. Gran fortaleza en el control	*80*

Cuando un riesgo tenga más de un control asociado, el porcentaje de mitigación se calculará mediante una media ponderada de los porcentajes de mitigación de dichos controles, considerando el peso que tenga cada control (ponderación).

Por otro lado, podría darse el caso de que desde un punto de vista de diseño, los controles asignados a un riesgo generen una gran fortaleza. Pero hay que evaluar si dichos controles finalmente se aplican tal y como fueron diseñados y/o si han tenido incidencias.

Si se detecta que los controles asociados a un riesgo generan incumplimientos, significará que el porcentaje de mitigación será menor que el inicialmente esperado. Por este motivo, el Motor de Cumplimiento rebajará el porcentaje de mitigación en un 50% cuando esta situación ocurra.

6.3.3 Parametrizando MC360: Asociación de las medidas y/o controles, a los riesgos

En la Matriz de Riesgos procederemos a asociar las medidas mitigadoras y controles a los riesgos identificados, de manera que nos permita parametrizar el MC360. Para ello, dentro de la matriz de Riesgo, en una tabla específica, relacionaremos los Riesgos y las medidas y controles relacionados.

- Ponderación: La Ponderación será la importancia que tenga esa medida o control dentro del Riesgo. Los posibles valores irán de 1 (menor importancia) a 10 (mayor importancia).

Un ejemplo de la tabla sería:

CodRiesgo	CodControl	Ponderacion
R165	C297	5
R166	C298	5

6.4 Identificación de las Evidencias (Datos) que soporten la aplicación de los controles y medidas mitigatorias

Para justificar que un control se ejecuta correctamente, o no, se le deberá asignar una o varias evidencias (Datos en MC360). Una evidencia podría ser la descripción de un control y/o una medida mitigante existente. También podría ser un manual u otra documentación. En ocasiones, será el resultado de la verificación por parte de Cumplimiento Normativo del funcionamiento de dicho control o medida mitigante.

Cuando definimos el Mapa de Riegos deberemos asignar a cada medida mitigadora o control la evidencia o evidencias de que dicho control se realiza o que existe la medida mitigadora que evita el riesgo. Para cada evidencia se deberá identificar:

Código de Evidencia (Dato)	Código único asignado al Control. Comenzará con una "**D**" y un número secuencial.
Nombre	Nombre corto de la evidencia (Dato)
Descripción	Descripción de la evidencia. Se incluye instrucciones de qué tipo de información hay que identificar para dar por válida la evidencia.
Requiere documento	Este campo indicará si la evidencia necesita de subir a la herramienta de cumplimiento (Motor de Cumplimiento 360) algún documento o no. Valores;: SI / NO.
Fuente (código)	Código de la Fuente que está a cargo de esta evidencia en el Motor de Cumplimiento,
Tipo	El control podrá ser numérico (se basa en un número resultado del control) o lógico (si/no, es decir, el control se realiza y cómo se realiza)
Unidades	Si el control es lógico, el valor asociado será SI/NO. SI es numérico, podrían ser: unidades o %.
Vigencia	Establece la vigencia máxima de la evidencia desde que se sube al Motor de cumplimiento. A partir de esa fecha, la evidencia se considerará no vigente.

6.4.1 Parametrizando MC360: Asociación de las evidencias (datos) a las medidas mitigatorias o controles

En la Matriz de Riesgos procederemos a asociar las evidencias a las medidas mitigadoras y controles a los riesgos identificados, de manera que nos permita parametrizar el MC360. Para ello, dentro de la matriz de Riesgo, en una tabla específica, relacionaremos los Riesgos y las medidas y controles relacionados.

Un ejemplo de la tabla sería:

CodControl	CodDato
C297	D242
C298	D243

6.5 Valoración del Riesgo Residual

Se trata del nivel de riesgo que permanece activo en nuestra Entidad, habiendo aplicado los controles diseñados para su prevención o inhibición. Esto es, el riesgo remanente tras efectuar su análisis. Esto permitirá a la Entidad definir qué escenarios son asumibles (riesgo residual), aplicando o mejorando los controles existentes, y cuales, en ningún caso, pueden ser tolerables.

Este riesgo deberá ser calculado para cada uno de los riesgos identificados, así como para la Sección en su conjunto.

Su cálculo se realiza mediante la aplicación de la siguiente fórmula:

Riesgo Residual = Riesgo Inherente – Efectividad (fortaleza) de los Controles (Mitigación)

La efectividad de los controles vendrá dada por el % de mitigación de los riesgos a los que están asociados. La fórmula anterior también podría expresarse de la siguiente manera:

Riesgo Residual = Riesgo inherente - % Mitigación de los controles.

El % de mitigación de los controles será la media ponderada de su mitigación, considerando el peso de cada control en el riesgo al que esté asociado.

Dado que el riesgo inherente tiene un rango de valoración entre 1 y 25, de igual forma el riesgo residual utilizará el mismo rango de valoración. Según los resultados obtenidos, el riesgo residual se encuadrará en estos posibles escenarios:

Categoría	Número	Valor Riesgo Residual %
Extremo	15 a 25	60% a 100%
Alto	9 y 14	36% a 59%
Moderado	6 y 8	24% a 35%
Bajo	4 y 5	16% a 23%
Muy bajo	1 y 3	1% a 15%

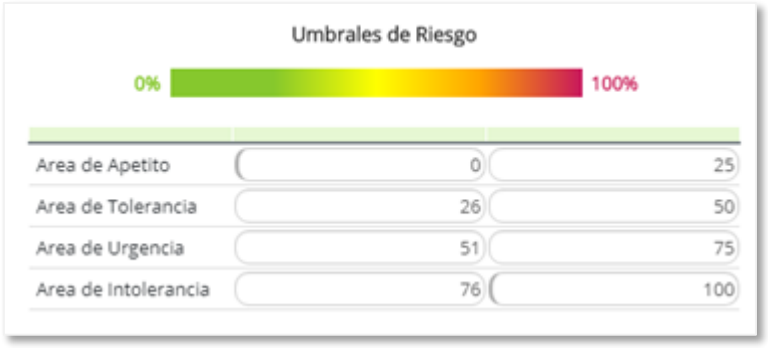
6.6 Determinar el nivel de riesgo aceptable o apetito al riesgo

Cuando ya han sido identificados los riesgos a los que la Entidad se enfrenta, la probabilidad de que estos se puedan llegar a materializar y el impacto que podrían causar, es el momento de determinar el grado de tolerancia que la Entidad tendrá a cada riesgo. Esto se conoce como el "apetito de riesgo" y hace referencia al nivel de riesgo que está dispuesta a asumir nuestra Entidad en la consecución de sus objetivos, permitiendo, además de optimizar el binomio riesgo-rentabilidad, mantener los riesgos dentro de los niveles deseados.

Esta metodología establece 4 umbrales de apetito de riesgo o intervalos de tolerancia y corresponden al porcentaje del grado de nivel de riesgo. Los 4 intervalos definidos por los umbrales tienen la siguiente denominación:

- *Área de Apetito (verde).*
- *Área de Tolerancia (amarillo).*
- *Área de Urgencia (naranja)*
- *Área de Intolerancia (rojo)*

El resultado obtenido en el riesgo residual se encuadrarán en uno de los 4 niveles definidos, mediante una representación gráfica como la que se adjunta:



Cada nivel implicará una serie de acciones a realizar por la Entidad con los riesgos evaluados, determinando el nivel de aceptación, o no, de ciertos riesgos. En este sentido, las acciones a realizar por la Entidad según el nivel serán:

- *Área de Apetito (verde)*. Este nivel implica que la Entidad asume como riesgo aceptable. Esto no implica que la Entidad no decida analizar la posibilidad de reforzar los controles existentes para obtener un mejor riesgo residual.
- *Área de Tolerancia (amarillo)*. Se analizarán los riesgos De manera discrecional, se podrá determinar que se asume un determinado riesgo, si el análisis del coste/beneficio de su mitigación no justifica la inversión necesaria.
- *Área de Urgencia (naranja)*. Los riesgos que se ubiquen en este nivel serán revisados para determinar qué tipo de acciones deben realizarse, especialmente los que se acerquen al intervalo de Intolerancia. Deberán establecerse los correspondientes planes de acción.
- *Área de Intolerancia (rojo)*. Todos los riesgos que caigan en este nivel, deberán ser tratados con urgencia, estableciéndose el correspondiente plan de acción.

Esta decisión sobre el nivel de riesgo aceptable o apetito de riesgo corresponde a la Comisión Mixta de Auditoría por delegación del Órgano de Gobierno.

Una vez aprobado el nivel de riesgo aceptable o apetito de riesgo, el órgano competente, en nuestro caso la Comisión Mixta de Auditoría, decidirá qué actuación debe realizarse con aquellos riesgos no aceptables o que están por encima del apetito de riesgo de la Entidad:

- *Asumir el riesgo* (aceptar, no se tratan).
- *Mitigar el riesgo* (reducir) implantando nuevos controles o mejorando los ya existentes.
- *Traspasar el riesgo a terceros* (transferirlo mediante seguros, contratación de proveedores, etc.).
- *Eliminar el riesgo* (evitar la actividad relacionada).

En todo caso, se deberán documentar las decisiones acordadas sobre cada uno de los riesgos identificados.

Si se ha decidido *mitigar los riesgos*, a la hora de seleccionar los controles, los responsables de las actividades de la Entidad junto con Cumplimiento Normativo, procurarán que exista un equilibrio entre controles organizativos y tecnológicos. Dichos controles pueden ser:

  - Sobre controles implantados, en los que se valorará el grado de madurez con respecto al riesgo a mitigar.
  - Sobre controles nuevos que no están implantados.

Para la identificación y selección de controles se toman en consideración diversos aspectos, entre los que destacan los siguientes:

- Facilidad para su implantación.
- Efecto del control sobre el responsable de la tarea, basado en que ayuda a realizar sus funciones de modo más eficiente.
- Modo en el que actúa el control sobre el riesgo (prevención o reacción).
- Medios disponibles para la implantación del control.

En todo caso, si se precisa, la Matriz de Riesgos de la Sección de Cumplimiento afectada deberá ser revisada para incluir o modificar los elementos que se vean afectados por el resultado de la revisión (riesgos, controles, evidencias,…).

En consecuencia, toda modificación de la matriz de riesgos, deberá ser ajustada en el Motor de Cumplimiento 360.

En línea con lo incluido en el Manual de Cumplimiento Normativo, una vez se haya finalizado la revisión de la Sección (Riesgo o Control), se creará el correspondiente informe por parte de Cumplimiento Normativo que será presentado al Comité de Auditoría. Sus resultados serán incluidos en los Informes periódicos que se realizan para la Dirección.

6.7 Definir el Plan de Acción

Una vez finalizada la revisión de una Sección de Cumplimiento y obtenidos los resultados, se identificarán los riesgos que hayan generado un mayor riesgo residual, los posibles incumplimientos asociados. Se analizará en qué umbrales de riesgo se han situado y que medidas deben tomarse.

Para cada incumplimiento detectado, se deberá analizar, en función del nivel de riesgo ubicado, qué acciones deben ponerse en marcha para solucionar los incumplimientos antes mencionados. Esto implicará, tal y como establece el Manual de Cumplimiento, que la Unidad de Cumplimiento Normativo deberá:

- Mantener una comunicación estrecha con la Unidad responsable de la actividad sobre la cual se ha lanzado el plan de acción, para monitorizar la implantación de la misma.

- A la fecha prevista de implantación, contactará con la Unidad responsable de la implantación para comprobar la finalización efectiva de la acción, pidiendo si es necesario, evidencias de dicha implantación.
- Si la acción ha sido completada satisfactoriamente, se dejará constancia de ello en el control de incumplimientos mantenido por la Unidad de Cumplimiento.
- Si la acción no ha sido completada, se debe registrar el motivo por que no se ha llevado a cabo, determinando nueva fecha de implantación y si es necesario, nuevos responsables de la misma

Los incumplimientos detectados, así como el resultado de su monitorización, serán incluidos en los informes periódicos que Cumplimiento Normativo elevará a los órganos de Dirección de la Entidad.

6.8 Determinación de la periodicidad de revisión de las Secciones de Cumplimiento

Es importante determinar, en función de su robustez, con qué periodicidad se debe revisar las Secciones de Cumplimiento. Esta información deberá ser considerada en el Plan de Trabajo Anual de la Unidad de Cumplimiento.

En nuestra metodología, cuando una Sección sea revisada, se determinará su nivel de riesgo residual y en función del resultado obtenido se identificará la periodicidad de revisión de dicha sección:

- *Área de Apetito (verde)*. En este caso, la sección se evaluará cada **3** años.
- *Área de Tolerancia (amarillo)*. Una sección que muestre un riesgo residual que lo ubique en esta área, implicará una revisión cada **2** años.
- *Área de Urgencia (naranja)*. Implicará una **revisión anual**.
- *Área de Intolerancia (rojo)*. Dado el nivel de intolerancia obtenido, implicará que en un plazo **entre 6 y 12 meses**, esta Sección deberá haber sido revisada para comprobar que los incumplimientos detectados han sido solventados.

7 Aprobación y revisión de la metodología

La presente Metodología ha sido aprobada por el Consejo Rector y en su caso, sus posteriores modificaciones serán aprobadas por la Comisión Mixta de Auditoría por delegación de dicho Órgano de Gobierno.

Esta metodología será revisada al menos una vez al año y en cualquier caso, cuando se tenga constancia que se ha producido alguna modificación importante.

8 HISTORIAL DE VERSIONES Y MODIFICACIONES

Versión	Secciones Afectadas	Descripción de la modificación	Autor	Fecha
Inicial	Todas	Versión Inicial	CN	30/07/2020
		Revisión anual	CN	30/09/2021