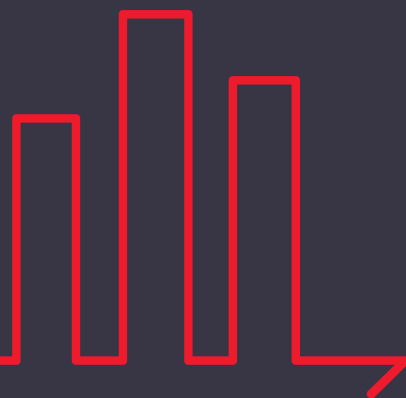


| GRUPO TOYOTA CAETANO PORTUGAL

# POLÍTICA DE GESTÃO DE RISCO



## ÍNDICE

|                                                                        |          |
|------------------------------------------------------------------------|----------|
| <b>1 – Objetivo</b>                                                    | <b>3</b> |
| <b>2 – Âmbito de Aplicação</b>                                         | <b>3</b> |
| <b>3 – Modelo de Governação da Gestão do Risco</b>                     | <b>3</b> |
| <b>4 – Processo de Gestão de Risco</b>                                 | <b>6</b> |
| 4.1 – Identificação dos riscos por tipologia                           | 7        |
| 4.2 – Avaliação dos riscos                                             | 7        |
| 4.3 – Resposta   Decisão sobre os riscos                               | 8        |
| 4.4 – Resposta   Definição das medidas de mitigação dos riscos a gerir | 8        |
| 4.5 – Monitorização das medidas/riscos                                 | 8        |
| 4.6 – Reporte   Comunicação e consulta/debate                          | 8        |
| 4.7 – Reporte   Suporte, supervisão e revisão                          | 8        |
| <b>5 – Apetite e Tolerância ao Risco</b>                               | <b>9</b> |
| <b>6 – Revisão da Política</b>                                         | <b>9</b> |
| <b>7 – Aprovação e divulgação</b>                                      | <b>9</b> |

## 1 – Objetivo

A presente Política de Gestão de Risco tem como objetivo estabelecer os princípios, processos e responsabilidades dos principais intervenientes do processo de gestão de risco que rege a identificação, avaliação, resposta, monitorização e reporte dos riscos que possam afetar a reputação e concretização dos objetivos estratégicos do Grupo Toyota Caetano Portugal, salvaguardando a proteção das pessoas, do ambiente e dos ativos.

Com a instituição da Política de Gestão de Risco, o Grupo pretende integrar e promover a gestão de risco no processo de tomada de decisões estratégicas e na gestão diária das operações. Com a sua implementação espera igualmente:

- otimizar a relação risco/retorno financeiro, potenciando assim oportunidades através de uma gestão proativa dos riscos, contribuindo para a permanente criação de valor pelo Grupo respeitando as expectativas dos *stakeholders* internos e externos;
- monitorizar e antecipar potenciais alterações de contexto interno e externo, estimando o seu impacto no negócio;
- reforçar o cumprimento dos requisitos legais e regulatórios a que está sujeito; e
- estar alinhado com as melhores práticas internacionais e normativos aplicáveis.

## 2 – Âmbito de Aplicação

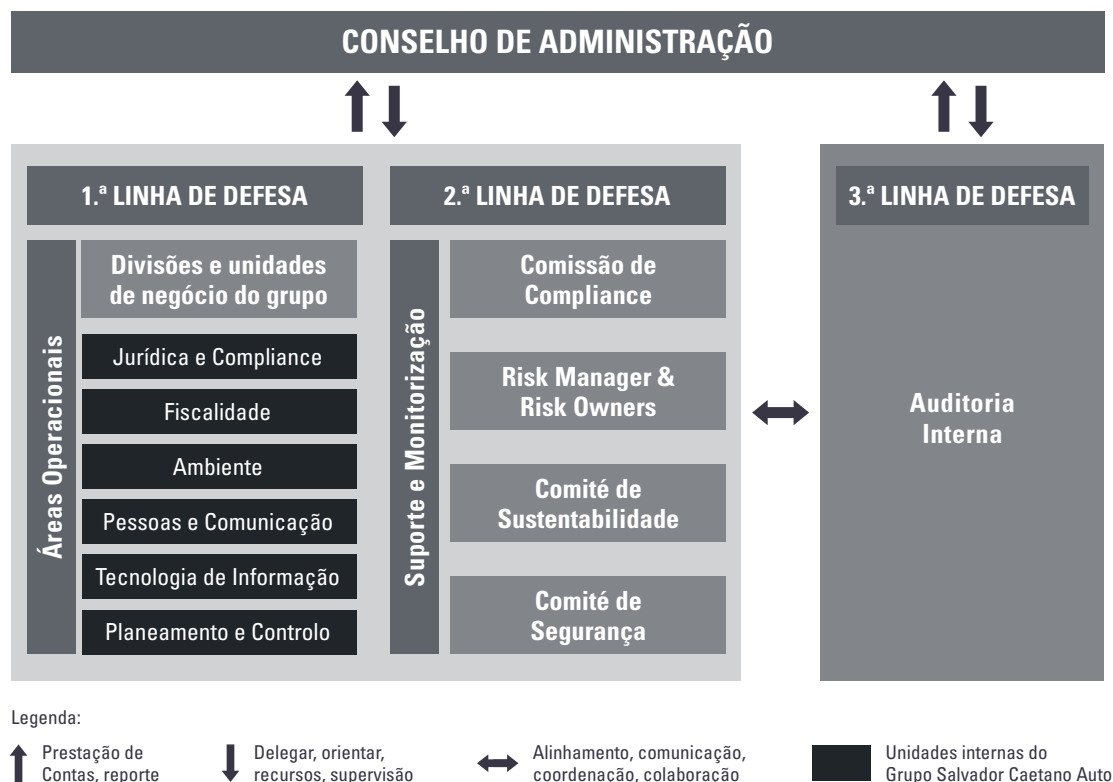
A presente política aplica-se a todas as empresas que integram o Grupo Toyota Caetano Portugal, independentemente da sua localização ou dimensão.

A gestão do risco deve ser assegurada por todas as Direções Gerais das divisões e unidades de negócio do Grupo, para garantir, em todos os níveis hierárquicos e atendendo à responsabilidade inerente a cada interveniente, uma maior consciência e ponderação na tomada de decisões e uma visão integrada dos riscos, alinhada com o apetite ao risco definido.

## 3 – Modelo de Governação da Gestão do Risco

O modelo de governo da gestão de risco do Grupo Toyota Caetano é fundamental para a formalização e estruturação da gestão de risco no Grupo, de forma a facilitar a fluidez e eficácia de todo o processo. O Modelo está baseado no conceito de Três Linhas de Defesa, que visa definir e responsabilizar os recursos apropriados à identificação, avaliação, resposta, monitorização e reporte dos riscos relevantes a que se encontra sujeito o Grupo.

Neste contexto, a estrutura formal do modelo é representada na figura seguinte:



Apresentam-se de seguida, as responsabilidades de cada interveniente no Modelo de Governo da Gestão de Risco do Grupo Toyota Caetano.

### Conselho de Administração:

- Promover uma cultura efetiva de gestão de risco transversal;
- Considerar a política de gestão de risco na definição dos objetivos estratégicos do Grupo Toyota Caetano supervisionando a sua execução;
- Aprovar a política de gestão de risco, modelo de governo e processo de gestão de risco a adotar e assegurar;
- Definir o apetite/tolerância ao risco;
- Assegurar que os principais riscos a que o Grupo Toyota Caetano se encontra exposto são identificados e reduzidos para níveis aceitáveis, em linha com o apetite e com a tolerância de risco definidos;

- Aprovar os planos de atividades no âmbito da gestão de risco;
- Apreciar o Relatório Anual de Gestão de Risco;
- Disponibilizar meios e recursos com vista à eficácia e eficiência da gestão de risco; e
- Acompanhar e rever o trabalho realizado pela Comissão de Compliance, *Risk Manager & Risk Owners*; Comité de Sustentabilidade e Comité de Segurança.

**Auditorias internas:**

- Avaliar a eficácia e efetividade do processo de gestão de risco, aconselhando e propondo as recomendações que se mostrem necessárias às 1ª e 2ª linhas de defesa;
- Planear e realizar auditorias baseadas no risco; e
- Realizar ações de follow-up de recomendações.

**Comissão de Compliance, *Risk Manager & Risk Owners*,  
Comité de Sustentabilidade e Comité de Segurança:**

Conscientes da existência de algumas sinergias entre estas quatro instâncias, cada uma delas tem um interlocutor delegado que garante a articulação da matéria relevante no âmbito do processo Gestão de Risco do Grupo com o *Risk Manager*. Todas as instâncias mencionadas, na sua área de especialização/intervenção, são responsáveis por:

- Definir e implementar a metodologia, o processo e os procedimentos para a gestão integrada de riscos;
- Planear e programar o ciclo anual do processo de gestão de risco;
- Elaborar os planos de atividade no âmbito da gestão de risco;
- Dinamizar e acompanhar o processo de identificação, análise, avaliação e resposta aos riscos;
- Alertar para potenciais riscos na definição dos objetivos estratégicos e operacionais;
- Elaborar a matriz dos top risks;
- Assegurar que se encontra implementado um processo efetivo de monitorização dos top risks;
- Assegurar a monitorização dos indicadores de risco definidos; e
- Assegurar o reporte periódico ao Conselho de Administração.

**Ao *Risk Manager* cabe, adicionalmente, a responsabilidade de:**

- Elaborar a Política de Gestão de Risco e propor revisões à mesma; e
- Identificar alterações que levem a uma revisão extraordinária do modelo de risco.

### **Divisões, Unidades de Negócio do Grupo Toyota Caetano e Unidades de suporte da Salvador Caetano Auto:**

- Identificação dos riscos;
- Participar no processo de análise, avaliação dos riscos e definir a estratégia de resposta ao risco (medidas de mitigação);
- Avaliar os custos da implementação de novas medidas de mitigação;
- Definir e implementar os planos de ação aprovados;
- Definir e monitorizar indicadores de risco;
- Cooperar, de forma permanente, com a Comissão de Compliance, o *Risk Manager* e *Risk Owner*, o Comité de Sustentabilidade e o Comité de Segurança no âmbito da gestão de risco; e
- Implementar as orientações e recomendações dadas pelo Conselho de Administração, Comissão de Compliance, *Risk Manager*, Comité de Sustentabilidade, Comité de Segurança e/ou de auditorias realizadas.

## **4 – Processo de Gestão de Risco**

O Processo de Gestão de Risco tem como referência o International Organization for Standardization 31000 – Risk Management (“ISO 31000”, 2018). É um processo iterativo de melhoria contínua, constituído pelas seguintes etapas: (i) identificação dos riscos por tipologia, (ii) avaliação do risco, (iii) decisão sobre o risco, (iv) definição das medidas de mitigação do risco a gerir e (v) monitorização do risco. As diferentes etapas são consolidadas por um processo de comunicação e consulta/debate e por um processo de suporte, supervisão e revisão (ver figura 2).

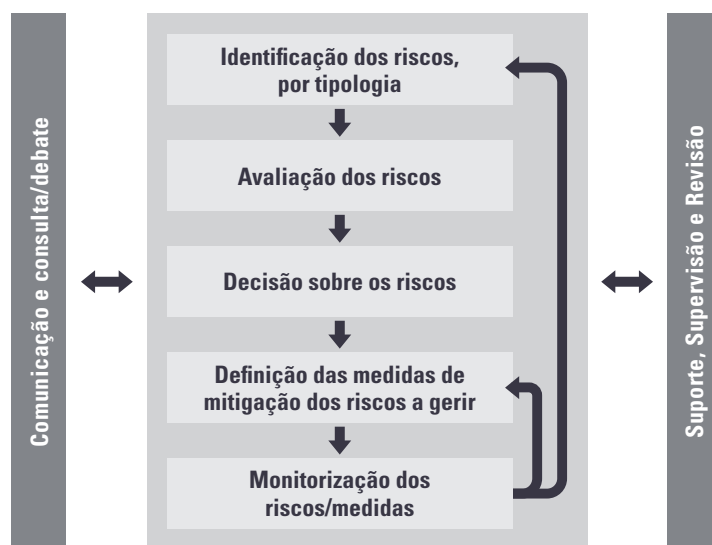


Figura 2 - Fases do processo de gestão de risco

#### **4.1 – Identificação dos riscos por tipologia**

Para que o processo de gestão de risco seja efetivo é necessário que o Grupo e inerentemente as suas divisões e unidades de negócio/suporte conheçam, a cada momento, os riscos a que estão, ou podem vir a estar, expostos, bem como as causas e efeitos que lhes estão associados.

Para o levantamento dos riscos que podem afetar a estratégia e desempenho dos negócios, deve ser utilizado um modelo de análise:

- *Top-down* (para identificação de riscos de natureza mais estratégico-tática); e
- *Bottom-up* (para identificação de riscos de natureza mais operacional).

Por esta via, o processo contempla:

- o alinhamento estratégico das unidades de negócio e do Grupo, com os riscos identificados; e
- o envolvimento e sensibilização de todos os colaboradores no processo de gestão de risco, na responsabilidade inerente a cada função.

O processo de identificação deve ter presente os diferentes tipos de risco a que uma organização pode estar sujeita. Nomeadamente:

- Riscos estratégicos
- Riscos legais e de conformidade
- Riscos reputacionais
- Riscos operacionais
- Riscos do capital humano
- Riscos financeiros
- Riscos tecnológicos
- Riscos ambientais e climáticos

Esta categorização auxilia o processo de identificação e direciona os negócios a gerir os riscos de uma forma sistematizada e estruturada.

#### **4.2 – Avaliação dos riscos**

A avaliação dos riscos identificados deve ser determinada com uma periodicidade mínima anual, hierarquizada e mapeada com base numa metodologia de Matriz de Risco. A Matriz de Risco faz a avaliação de cada risco, a diferentes níveis, considerando:

- a sua probabilidade de ocorrência num determinado período; e
- a magnitude do impacto que o mesmo pode provocar.

O nível de criticidade de cada um dos riscos e respetiva análise de sensibilidade é determinada pelo cruzamento dos dois fatores e respetivo mapeamento na Matriz de Risco correspondente, a qual reflete, no final, a importância relativa de cada deles.

### **4.3 — Resposta | Decisão sobre os riscos**

Em função do mapeamento e hierarquização dos riscos identificados com base na Matriz de Risco, é necessário decidir como atuar sobre cada um dos riscos. Nomeadamente, decidir entre aceitar o risco (porque é residual/insignificante, p.e.), transferir o risco (p.e. fazendo um seguro), mitigar ou eliminar o risco (definindo ações de mitigação/eliminação do mesmo).

Note-se que o sistema de gestão de risco não tem como objetivo eliminar completamente o risco das atividades do Grupo, mas sim avaliar o nível de risco e assegurar que são desenvolvidos todos os esforços para que o risco seja gerido de forma adequada, maximizando as oportunidades potenciais e minimizando os seus efeitos adversos.

### **4.4 — Resposta | Definição das medidas de mitigação dos riscos a gerir**

Para os riscos cuja decisão seja mitigar ou eliminar, é necessário que cada negócio defina as ações que irá desenvolver para o conseguir, respetivo plano e responsável interno.

### **4.5 — Monitorização das medidas/riscos**

Como mecanismo de controlo da execução das medidas de gestão de risco adotadas e da sua eficácia, a exemplo do que acontece com as restantes ações/projetos de gestão, devem ser identificados o(s) respetivo(s) indicador(es) para que sejam monitorizados por cada linha de defesa na respetiva periodicidade. Este processo funcionará como instrumento de alerta a desvios, permitindo antecipar as mudanças necessárias de forma a melhorar ou retomar a eficácia da(s) respetiva(s) medida(s) de mitigação/eliminação do risco.

### **4.6 — Reporte | Comunicação e consulta/debate**

O processo de gestão de risco do Grupo dispõe de mecanismos internos de comunicação e consulta/debate sobre as diversas componentes e questões associadas do sistema de alerta do risco, assim como um processo de comunicação estruturada dos riscos e medidas aos decisores.

### **4.7 — Reporte | Suporte, supervisão e revisão**

Além da promoção de iniciativas de formação e comunicação regulares com o objetivo de fomentar a cultura de risco em todos os níveis organizacionais, o Grupo dispõe de uma estrutura interna de suporte, disponível para ajudar em caso de dúvidas, análises e eventuais revisões associadas ao processo de Gestão de Risco. A mesma estrutura promove reuniões periódicas de monitorização ao processo das diferentes divisões e unidades do Grupo, organizadas por tipologia de risco (2ª linha de defesa). A supervisão e revisão é adicionalmente reforçada pela 3ª linha de defesa assegurada pela auditoria interna.



## **5 – Apetite e Tolerância ao Risco**

O Conselho de Administração define o apetite e tolerância ao risco do Grupo Toyota Caetano em função do impacto do mesmo nos resultados consolidados do Grupo e da sua cultura de maior aversão ou agressividade ao risco. As amplitudes de variação dos indicadores de cada risco auxiliam à análise e eventual ajuste/revisão dos mesmos. Esta definição assegura igualmente a coerência do Grupo nos mais relevantes processos de negócio e de decisão como parte integrante do desenvolvimento estratégico, decisões de investimento e do plano de negócios, por exemplo.

## **6 – Revisão da Política**

As revisões e alterações a efetuar à Política de Gestão de Risco são da competência do *Risk Manager*. Tais revisões ou alterações devem ser submetidas à apreciação e aprovação do Conselho de Administração.

O Grupo Toyota Caetano compromete-se a rever periodicamente a sua Política de Gestão de Risco e a atualizá-la sempre que as circunstâncias o justifiquem.

## **7 – Aprovação e divulgação**

A Política de Gestão de Risco entra em vigor com a sua aprovação em Conselho de Administração da Toyota Caetano Portugal. Sendo divulgada a todos os colaboradores e público em geral pela sua publicação na Intranet do Grupo e nos sítio web da Toyota Caetano Portugal.

A presente Política foi aprovada pelo Conselho de Administração da Toyota Caetano Portugal, S.A. em 16 de setembro de 2025.