NT-025

MANUAL DE CONTROLO INTERNO

Norma Transversal

Aprovado em reunião do Conselho de Administração de 23-10-2020

Índice

1. Objeto e âmbito de aplicação

1.1. O presente manual estabelece os princípios gerais e os requisitos das componentes do controlo interno, bem como o modelo organizacional associado à gestão integrada e transversal do controlo interno na Galp, entendido como o conjunto de processos executados pelos órgãos sociais, comissões especializadas, auditor interno e pelos/as colaboradores/as da Galp, com vista a conferir garantia razoável do cumprimento dos objetivos da Galp relacionados com as operações, reporte e conformidade.

1.2. O presente manual segue o modelo de referência COSO - *Internal Control Integrated Framework*. A Galp adota as cinco componentes deste modelo enquanto pilares do seu sistema de controlo interno: 1. Ambiente de controlo; 2. Avaliação de risco; 3. Atividades de controlo; 4. Informação e Comunicação; 5. Atividades de monitorização.

1.3. O desenho e implementação dos controlos nos processos regem-se pelo presente manual, e observam o disposto nos normativos transversais e setoriais da Galp em vigor.

1.4. Ficam abrangidas no âmbito de aplicação do presente manual todas as Unidades Organizacionais (UO) da Galp e sociedades participadas ou outras entidades, independentemente da sua natureza jurídica, em que a Galp detenha o controlo da sua gestão, englobando todas as geografias em que a Galp opera.

1.5. Nos casos em que a Galp não detenha direta ou indiretamente 100% do capital social da sociedade, as pessoas por aquela designadas para cargos de administração nessas entidades devem assegurar a aprovação e adoção da presente norma pelos respetivos órgãos de administração.

1.6. As pessoas designadas pela Galp para cargos de administração nas empresas associadas em que a Galp não detenha o controlo da sua gestão devem realizar esforços para promover nessas sociedades as medidas conducentes ao reconhecimento e adoção do presente Manual ou de regras equivalentes.

2. Componentes do controlo interno

As componentes do controlo interno atuam e operam de forma integrada e interdependente, como um sistema único, com o propósito de conferirem uma garantia razoável sobre o cumprimento dos objetivos da Galp em relação (i) à prossecução dos seus objetivos estratégicos, (ii) à preparação e divulgação de informação financeira e não financeira a fornecer às partes interessadas internas e externas; (iii) ao cumprimento da lei e normativos aplicáveis; (iv) à salvaguarda e proteção dos ativos; e (v) à eficiência e eficácia nas operações.

As cinco componentes são interdependentes com uma multiplicidade de inter-relações e ligações entre si, particularmente na forma como os princípios em que assentam as componentes interagem entre si.

A Galp reconhece que o controlo interno se encontra sujeito a limitações que resultam fundamentalmente de:

- eventual falta de clareza dos objetivos estratégicos da Galp definidos;
- realização por pessoas de tarefas, atividades de controlo e tomada de decisões, que estão por isso sujeitas a erros, falhas ou enviesamento;
- caracterização de conduta fraudulenta, tal como conluio e capacidade da gestão de topo em ultrapassar os controlos existentes;
- eventos externos que possam transcender a capacidade de controlo da Galp.

Estas limitações determinam a impossibilidade de o controlo interno conferir uma garantia absoluta sobre o cumprimento dos objetivos da Galp, permitindo antes conferir uma garantia razoável.

2.1 Componente 1: ambiente de controlo

O ambiente de controlo consiste no conjunto de normas, processos e estruturas de que a Galp dispõe e que constitui a base do seu sistema de controlo interno.

O ambiente de controlo é influenciado por fatores internos e externos, como sejam os valores da Galp e o mercado em que se integra, refletindo o posicionamento dos órgãos de gestão face à importância do sistema de controlo interno e orientando todos/as os/as colaboradores/as na tomada de decisões numa ótica de controlo.

O ambiente de controlo é apoiado pela cultura organizacional, que deve assegurar que as expetativas de comportamento que refletem um compromisso com valores éticos, responsabilidades, políticas, normas e procedimentos sejam realizadas. A gestão de topo estabelece e comunica a importância do controlo interno e os padrões de conduta esperados.

2.1.1 Princípios

O ambiente de controlo da Galp assenta nos seguintes cinco princípios:

1 – Demonstração de compromisso em relação aos valores éticos

O Conselho de Administração, Conselho Fiscal, Comissão Executiva, UO e comissões especializadas da Galp demonstram compromisso em relação aos valores éticos através da emanação das seguintes diretrizes, ações, comportamentos e documentos:

- Visão e Valores da Galp (disponíveis na intranet da Galp e no site oficial neste link);
- Código de Ética e Conduta (disponível na intranet da Galp e no site oficial neste link);
- Políticas, normas e procedimentos (divulgados e acessíveis na intranet da Galp neste link);
- Canal de comunicação de irregularidades (através do endereço opentalk@galp.com ou de formulário disponibilizado na intranet e no site oficial da Galp neste link);
- Existência de processo de averiguação de irregularidades pela Comissão de Ética e Conduta nos termos do procedimento aplicável (disponível na intranet e no site oficial da Galp neste link).

Estas diretrizes, ações, comportamentos e documentos são comunicados internamente a todos os níveis da Galp, e externamente aos *stakeholders,* incluindo prestadores de serviços e parceiros de negócio. Os responsáveis pela relação com estes *stakeholders* externos asseguram a obtenção do compromisso formal por parte dos mesmos.

A Galp exige, de todos os seus colaboradores e outros intervenientes no sistema de controlo interno, atitudes de integridade, padrões éticos elevados, liderança, pensamento crítico e capacidade de resolução de problemas.

Qualquer comportamento não consistente com padrões de conduta, políticas, práticas e responsabilidades de controlo interno que seja identificado, é avaliado, e são tomadas as medidas de correção em tempo útil.

2 – Independência do Conselho de Administração face à Comissão Executiva e supervisão do desenvolvimento e desempenho do Controlo Interno pelo Conselho de Administração e Conselho Fiscal

O Conselho de Administração é responsável pela aprovação da política do sistema de controlo interno e definição da estratégia e supervisão da gestão do risco, acompanhando e controlando o desempenho das funções delegadas na Comissão Executiva, em particular no desenvolvimento e desempenho do controlo interno.

A gestão corrente da Sociedade é exercida pela Comissão Executiva nos termos da delegação de poderes conferida pelo Conselho de Administração, disponível no Regulamento deste órgão (acessível

na intranet e no site oficial da Galp neste link), o qual supervisiona e acompanha a gestão, inclusive através dos seus membros independentes.

Ao Conselho Fiscal cabe o papel de fiscalizar a eficácia dos sistemas de gestão de riscos, de controlo interno e de auditoria interna e externa, e propor os ajustamentos necessários, bem como o de avaliar anualmente o seu funcionamento e os respetivos procedimentos internos e pronunciar-se sobre os planos de trabalho e os recursos afetos aos serviços de controlo interno, conforme previsto no seu Regulamento (disponível no site oficial da Galp e na intranet neste link).

Cabe à Comissão Executiva pronunciar-se junto do Conselho Fiscal, sobre a eficácia operacional do controlo interno, em especial do SCIRF, com base nas conclusões dos testes independentes realizados pela função de auditoria interna.

3 – Definição pela Comissão Executiva, com supervisão do Conselho de Administração, da estrutura, linhas de reporte, níveis de competência e de responsabilidade necessários a alcançar os objetivos da Galp

A estrutura organizativa da Galp assenta, por um lado, em unidades de negócio e, por outro, num centro corporativo composto por funções de suporte. As responsabilidades e competências são atribuídas pela Comissão Executiva através da aprovação de normas orgânicas sob a coordenação de cada um dos administradores executivos.

A área corporativa responsável pelo desenvolvimento organizacional da Galp é responsável pela atribuição de competências individuais de acordo com a norma interna aplicável, e ainda pela otimização e adequação das estruturas organizativas à estratégia definida, identificando oportunidades e prioridades de melhoria na estrutura organizacional da Galp, conforme definido em norma orgânica. A área corporativa responsável pelo *governance* da Galp formaliza as regras de tomada de decisão pela gestão e a atribuição de competências de representação perante terceiros, conforme estabelecido em norma orgânica.

As regras e os limites de competência a serem observados pelos colaboradores e titulares de órgãos com responsabilidade de decisão e vinculação na Galp encontram-se definidos em normas internas (disponíveis na intranet da Galp neste link).

A área corporativa responsável pelo controlo interno da Galp estabelece as orientações em matéria de estrutura, linhas de reporte, níveis de competência e de responsabilidade, necessários para o desenvolvimento de um sistema de controlo interno eficaz na Galp, em especial no que respeita ao SCIRF, conforme definido em norma orgânica, integrando o modelo de governo do controlo interno do relato financeiro na Galp (que pode ser acedido aqui).

A eficiência e eficácia das linhas de reporte e dos níveis de competência e responsabilidade no apoio ao sistema do controlo interno é periodicamente avaliada, conduzindo às revisões necessárias tendo em consideração as seguintes variáveis:

- Tipo de negócio, dimensão e distribuição geográfica das UO;
- Risco relacionado com os objetivos da Galp e dos processos de negócio;
- Natureza da atribuição de competências e responsabilidade para a gestão de topo, UO, funcionais e gestão geográfica; e
- Requisitos financeiros, legais, regulamentares e tributários.

4 – Demonstração de compromisso para atrair, desenvolver e reter competência, em linha com os objetivos da Galp

A Comissão Executiva supervisiona a avaliação das competências existentes na Galp face às políticas definidas para cumprimento dos objetivos, realizando uma análise custo/benefício de diferentes níveis de competências e experiência.

O processo de avaliação de desempenho em vigor na Galp assegura a validação dos resultados pelos níveis hierárquicos superiores, de forma sucessiva até aos seus administradores executivos.

As competências avaliadas são técnicas (de conhecimento) e comportamentais, estas corporizadas nos valores da Galp, para os quais estão descritos comportamentos pretendidos e escalas de observação.

Para além da avaliação de competências, a avaliação de desempenho inclui o atingimento de resultados associados a métricas de empresa, equipa e individuais, as quais estão diretamente ligadas aos objetivos e resultados da Galp.

O resultado global da avaliação de desempenho contribui para o apuramento da remuneração variável.

A área corporativa responsável pela gestão dos colaboradores/as da Galp dirige os processos necessários para atrair, desenvolver e reter colaboradores competentes, em número suficiente para suportar a prossecução dos seus objetivos, de acordo com políticas e normas definidas, designadamente a norma de recrutamento e mobilidade (que pode ser acedida aqui).

5 – Atribuição de responsabilidades aos intervenientes no controlo interno adequadas a alcançar os objetivos da Galp

A Comissão Executiva atribui responsabilidades pelo desempenho do controlo interno a todos os níveis da organização através da definição de normas orgânicas das respetivas áreas. A atribuição das responsabilidades macro encontra-se descrita na matriz de responsabilidades constante do ponto 5 deste Manual.

2.2 Componente 2: avaliação do risco

A avaliação do risco é um processo dinâmico e iterativo, no sentido em que depende dos objetivos da Galp, que podem ser alterados, e constitui a base para determinar como são tratados os riscos para o cumprimento desses objetivos.

2.2.1 Princípios

A avaliação de risco na Galp assenta nos seguintes princípios:

a) Identificação dos objetivos estratégicos, que são comunicados ao mercado (em especial, no âmbito do *Capital Markets Day* e através do Relatório de Gestão e Contas) e que permitem a identificação e avaliação dos riscos relativos ao seu cumprimento;

b) Identificação e análise dos riscos inerentes ao cumprimento dos objetivos da Galp como base para a determinação da forma como os riscos devem ser geridos. A identificação e avaliação dos riscos é realizada pelas primeira e segunda linhas de defesa da Galp nos termos da Política de Gestão de Risco da Galp (link), do modelo de governo de gestão de risco (link) e da norma interna de gestão de riscos em processos (link).

c) Consideração da possibilidade de fraude na avaliação dos riscos. A prevenção de fraude deve ser objeto de um programa específico de acordo com os princípios previstos no capítulo 3.2 do presente Manual;

d) Identificação e avaliação de alterações que possam impactar significativamente no sistema de controlo interno, tendo esta atribuição sido conferida ao Comité de Gestão de Risco por norma orgânica (disponível na intranet da Galp neste link).

2.2.2 Fases

A avaliação de risco na Galp no âmbito do sistema de controlo interno envolve cinco fases:

a) Identificação de objetivos – Identificação do contexto e dos objetivos principais do processo relevantes para fins de controlo interno;

b) Identificação e análise dos riscos – Identificação e análise dos riscos associados ao cumprimento dos principais objetivos e do processo;

c) Avaliação de riscos – Avaliação do grau de severidade dos riscos identificados, utilizando os critérios de impacto (i.e. reduzido, moderado, elevado ou muito elevado) e de probabilidade de ocorrência (i.e. remota, improvável, provável ou frequente);

d) Tratamento dos riscos – Em função da tolerância definida para os riscos, identificação e implementação da opção adotada para o tratamento do risco. A tolerância para os riscos é proposta pela Direção de Gestão de Risco e aprovada anualmente pelo Conselho de Administração, após parecer do Conselho Fiscal, sendo incorporada nos processos da Galp em conformidade com a norma interna de gestão de riscos em processos;

e) Monitorização dos riscos – Monitorização, através da supervisão realizada no âmbito das atividades de controlo estabelecidas, dos riscos quanto à eficácia das medidas de mitigação identificadas e quanto à evolução da exposição ao risco.

2.2.3 Sempre que a avaliação de riscos concluir por uma exposição superior à tolerância definida pela Galp, deve ser tomada decisão sobre a necessidade de criação ou intensificação da utilização de mecanismos de controlo para mitigação de risco identificado.

2.2.4 Os principais riscos e fatores de risco da indústria em que a Galp se integra, assim como os que são específicos da Galp encontram-se identificados, de forma sistematizada e organizada no Dicionário de Riscos da Galp (que pode ser consultado aqui).

2.3 Componente 3: atividades de controlo

As atividades de controlo (ou "controlos") consistem em ações definidas e implementadas que permitem mitigar os riscos a um nível considerado aceitável, tendo em conta o resultado do trabalho realizado na componente de avaliação de risco.

2.3.1 Princípios

Os princípios das atividades de controlo da Galp são os seguintes:

a) Seleção e desenvolvimento de atividades de controlo que contribuam para mitigar até um nível considerado aceitável os riscos de cumprimento dos objetivos da Galp;

b) Seleção e desenvolvimento de atividades de controlo sobre a tecnologia de suporte à prossecução dos seus objetivos;

c) Desenvolvimento de atividades de controlo definidas em normas internas que estabeleçam as condutas esperadas e procedimentos que as concretizam.

2.3.2 Tipologia

As atividades de controlo são caracterizadas em três grandes grupos:

- **Controlos de alto nível (*Entity level controls)*** – controlos pervasivos ("*tone-from-the-top*") e que constituem a base do sistema de controlo interno da Galp (ambiente de controlo). Estes controlos foram descritos no capítulo 2.1 do presente Manual.

- **Controlos gerais informáticos (*IT level controls*)** – controlos relacionados com a tecnologia de suporte à prossecução dos objetivos da Galp e com os respetivos processos. A conceção, implementação e funcionamento destas atividades de controlo é da responsabilidade da área corporativa de sistemas de informação ("IT & Digital"). A utilização de controlos gerais informáticos pela Galp encontra-se descrita no capítulo 3.5 deste Manual.

- **Controlos nos processos (*Process level controls*)** – controlos implementados nos processos de negócio, quer ao nível das áreas corporativas quer das unidades de negócio. A conceção, implementação e funcionamento destas atividades de controlo é da responsabilidade dos responsáveis pelos processos.

  As atividades de controlo interno na Galp devem encontrar-se documentadas ao nível dos processos, os quais são organizados de acordo com o Modelo de Processos da Galp, sendo suportados por plataforma SI, na qual são caracterizados os processos e os respetivos riscos e garantida a associação dos controlos ao fluxo do processo. Complementarmente, no que respeita ao SCIRF, os riscos de distorção com impacto no relato financeiro e as atividades de controlo desenhadas para mitigar tais riscos, serão documentadas em matriz de riscos e controlos em plataforma de SI, com caracterização dos controlos de alto nível, dos controlos gerais informáticos e dos controlos processuais. O mapeamento de processos na Galp é realizado de acordo com a norma interna relativa às regras de mapeamento de processos (disponível aqui).

2.3.3 Orientações e diretrizes

Na seleção, definição e implementação das atividades de controlo são consideradas as seguintes orientações e diretrizes, bem como os seus efeitos e limitações:

1. **Responsabilidade** – As atividades de controlo têm um responsável com a responsabilidade por reportar (*accountability*) sobre o seu funcionamento e eficácia. A indefinição na atribuição de responsabilidade por um controlo pode implicar redução da sua eficácia.

2. **Rastreabilidade** – É assegurada a manutenção de provas adequadas da execução dos controlos, documentais ou informáticas, por um período de tempo não inferior a cinco anos, sem prejuízo da política de retenção de informação aplicável. A ausência de rastreabilidade pode impedir a realização de um controlo subsequente ou a verificação da sua execução por parte de um terceiro independente.

3. **Ação preventiva ou corretiva** – As atividades de controlo traduzem-se em ações preventivas ou corretivas com o objetivo de limitar a probabilidade de ocorrência ou o impacto do risco, respetivamente.

4. **Eficácia** – Um controlo só alcança o seu objetivo de mitigar o risco se for eficaz, sendo a verificação desta eficácia parte do processo de monitorização. Deve ser dada maior preponderância a atividades de controlo com maior eficácia inerente. Assim, as atividades de controlo preventivas e automáticas (realizadas com recurso a meios tecnológicos/informáticos) devem ser privilegiadas face a atividades de controlo corretivas e manuais, devendo atender-se ao custo/benefício das opções possíveis.

5. **Complementaridade entre prevenção e deteção** – A maior eficácia associada às atividades preventivas deve ser complementada com atividades de controlo específicas de deteção e correção, em particular quando as situações que podem ultrapassar a eficácia da prevenção possam assumir impactos elevados.

6. **Segregação de funções** – Deve ser assegurada uma adequada segregação entre as atividades de controlo preventivas (exemplo: aprovações) e detetivas (exemplo: revisão) relacionadas com o mesmo risco. Neste sentido, a título exemplificativo, as revisões devem ser realizadas por um "terceiro independente" daquele que realizou a atividade preventiva.

7. **Segregação de acessos** – Os acessos lógicos ou físicos associados a mecanismos, sistemas ou tecnologias que suportam as atividades de controlo devem ser diferenciados de acordo com a segregação de funções definida.

8. **Periodicidade** – Uma maior frequência na execução de um controlo aumenta a sua eficácia. No entanto, esta não deve exceder a frequência com que a fonte que lhe está associada ocorre no processo (exemplo: o controlo de revisão de faturas emitidas deve ter uma periodicidade máxima correspondente à frequência de emissão das faturas).

9. **Dependência de tecnologia** – Quanto maior for a utilização de tecnologia maior o nível de confiança no controlo executado por se tornar menos suscetível de ser afetado por erros humanos. Contudo, a utilização de atividades de controlo com base em tecnologias ou

sistemas de informação deve ser adequadamente suportada por controlos informáticos específicos que mitiguem os riscos específicos relacionados com:

a) Infraestrutura tecnológica e operações;
b) Segurança;
c) Ciclo de vida das tecnologias de informação e comunicação; e
d) Prestadores de serviços.

2.3.4 Caracterização das atividades de controlo

As atividades de controlo na Galp são caracterizadas quanto à finalidade, tipologia, grau de automatização e periodicidade.

Finalidade – Caracterização quanto ao objetivo da atividade de controlo baseado nas asserções (objetivos da atividade de controlo):

- Autorização e aprovação – confirma a validade de uma determinada transação ou operação;
- Verificação – compara um ou mais elementos com uma determinada referência (definida, por exemplo, em norma interna ou manual) com o objetivo de identificar e tratar exceções. As verificações incidem normalmente sobre a plenitude, validade e exatidão das transações processadas. À informação objeto de verificação estão associadas uma ou mais grandezas de cariz monetário, físico, químico ou outro (exemplo: valor monetário, tempo, temperatura).
- Inventariação física – custódia, proteção ou conservação de ativos físicos (exemplos: equipamento, inventários, dinheiro e outros ativos físicos) e a sua contagem periódica e comparação com os montantes constantes dos registos.
- Salvaguarda de informação – controlos sobre o processamento, atualização e manutenção da plenitude, validade e exatidão dos dados e informação que suportam o processamento das transações (exemplo: dados mestre).
- Reconciliação – comparação entre dois ou mais elementos com o objetivo de tratar as exceções, de modo a eliminar divergências identificadas e assegurar a plenitude e a exatidão do processamento das transações.
- Revisão e supervisão – confirmação em como as outras atividades de controlo transacionais estão a ser executadas, em particular as autorizações/aprovações, as verificações, as inventariações físicas, as reconciliações e os controlos sobre salvaguarda de informação, estão a ser executadas integralmente, corretamente e de acordo com as políticas e procedimentos

da Galp. Estas atividades incidem particularmente em atividades com maior nível de risco associado e habitualmente envolvem apreciação crítica na sua seleção e execução.

Tipologia – Caracterização quanto ao momento de atuação das atividades de controlo:

- Preventivas – atuam antes do evento de risco, sendo concebidas e implementadas para prevenir a ocorrência de um evento ou resultado não intencional. Estes controlos têm a capacidade de reduzir a probabilidade de ocorrência de um determinado evento, conseguindo eliminar ou mitigar uma fonte de risco;

- Detetivas – atuam durante ou após a concretização do risco, sendo concebidas e implementadas para revelar um evento após a sua concretização, mas antes do objetivo principal se encontrar concluído ou comprometido. Estes controlos atuam fundamentalmente sobre uma ou mais dimensões de impacto, devendo desencadear uma ou mais ações corretivas ou mitigadoras do impacto.

Grau de automatização – Caracterização quanto à tecnologia que suporta a execução da atividade de controlo e que, no caso dos controlos automáticos ou semiautomáticos, identifica ainda os sistemas que intervêm na sua execução:

- Manuais – são executados manualmente e não requerem/dependem de tecnologia/sistemas de informação;

- Semiautomáticos – são executadas manualmente, porém requerem o envolvimento/dependência de tecnologia/sistemas de informação;

- Automáticos – são executados na sua totalidade através da utilização de tecnologia/sistemas de informação.

Periodicidade – caracteriza os controlos quanto à frequência da sua execução (exemplo: diariamente, semanalmente, mensalmente, trimestralmente, anualmente, *on-event*, ou seja, controlos executados sempre que exista essa necessidade).

O responsável pode ainda caracterizar os controlos quanto a outros aspetos, como seja o grau de cobertura do risco (exemplo: elevado, médio, baixo).

2.4 Componente 4: informação e comunicação

A presente componente do controlo interno consiste no conjunto de informação necessária à execução das tarefas de controlo interno adequadas a suportar o cumprimento dos seus objetivos e sua respetiva comunicação.

2.4.1 Princípios

A informação e comunicação no âmbito do controlo interno da Galp assentam nos seguintes princípios:

a) Obtenção, geração e utilização de informação de qualidade e relevante de suporte ao funcionamento do controlo interno;

b) Comunicação interna de informação, incluindo os objetivos e as responsabilidades, necessárias ao funcionamento do controlo interno;

c) Comunicação aos *stakeholders* de matérias relativas ao funcionamento do controlo interno.

2.4.2 Informação

Toda a informação necessária para o adequado funcionamento do sistema de controlo interno da Galp deve estar disponível, permitindo que as responsabilidades definidas em cada uma das cinco componentes do controlo interno possam ser exercidas de forma eficaz, e deve ser consistente com a necessidade que a Galp tem de avaliar e responder ao risco.

A informação deve estar disponível para quem dela necessite para exercer as suas atribuições no âmbito do controlo interno. Esta informação inclui os objetivos estratégicos da Galp, as políticas, normas, procedimentos específicos ou dados subjacentes à realização dos controlos.

A qualidade da informação implica a verificação dos seguintes requisitos:

- Plenitude;
- Exatidão;
- Validade;
- Adequação do conteúdo;
- Oportunidade;
- Atualidade;
- Facilidade de acesso.

Por outro lado, a informação deve respeitar as normas da Galp sobre segurança da informação (disponíveis na intranet da Galp neste link), proteção de dados pessoais (disponíveis na intranet da Galp neste link) e outras normas ou legislação aplicável ao longo do ciclo de vida da informação.

As atividades de controlo são objeto de informação documentada, a qual deve ser gerida e mantida em adequado estado de preservação e estar acessível, nomeadamente para efeitos dos

correspondentes processos de auditoria, interna ou externa, e de modo a assegurar o cumprimento do normativo transversal e setorial aplicável.

A informação relativa ao sistema de controlo interno é necessária para evidenciar a sua eficácia, para permitir uma monitorização adequada e para suportar a comunicação com os *stakeholders*, podendo existir em múltiplos formatos e estar ou não suportada em sistemas de informação.

As áreas corporativas responsáveis pelo controlo interno, pelo *governance* e *compliance,* pela gestão de risco, pela segurança dos sistemas de informação e pela segurança e sustentabilidade, devem ser informadas sobre a existência de insuficiências ao nível da informação necessária para o desempenho das responsabilidades atribuídas de controlo interno ou limitação relevante para a eficácia do controlo, de modo a que possam adotar ou propor as medidas adequadas para superar essas limitações.

2.4.3 Comunicação

A comunicação no controlo interno visa transmitir eficazmente:

- os objetivos da Galp;
- a importância e a pertinência de um sistema de controlo interno eficaz;
- o apetite ao risco e a respetiva tolerância;
- as normas aplicáveis ao controlo interno;
- o dicionário de riscos da Galp;
- as funções e responsabilidades dos intervenientes no controlo interno.

Os princípios de comunicação na Galp encontram-se previstos na Política de Comunicação (disponível no site oficial da Galp e na intranet neste link), cabendo à área corporativa responsável pela comunicação, a gestão da comunicação interna e externa da Galp, conforme atribuições conferidas em norma orgânica.

Todos os intervenientes no sistema de controlo interno devem ter conhecimento das suas responsabilidades e da forma como o seu desempenho se relaciona com o dos outros, sabendo reconhecer de forma atempada um problema, determinar a sua causa e definir uma medida corretiva apropriada.

O mesmo deve acontecer na comunicação com *stakeholders* externos, assegurando a dinâmica necessária à compreensão da evolução dos fatores relevantes para o sistema de controlo interno.

2.5 Componente 5: atividades de monitorização

A monitorização do controlo interno consiste na verificação, interna ou independente, da aplicação e eficácia dos controlos definidos.

2.5.1 Princípios

As atividades de monitorização do controlo interno da Galp assentam em dois princípios:

a) Definição, desenvolvimento e realização de análises correntes e/ou pontuais para verificar se as componentes do controlo interno funcionam;

b) Avaliação e comunicação, em tempo útil, às partes responsáveis por tomar as ações corretivas adequadas, de deficiências do controlo interno detetadas, incluindo aos órgãos sociais.

2.5.2 Objetivos

As atividades de monitorização devem ser realizadas com uma periodicidade adequada face ao nível de risco que os controlos pretendem mitigar e têm como objetivos:

a) Assegurar que os controlos existentes são efetivos, eficientes e eficazes, tanto no desenho como na sua implementação e eficácia operacional;

b) Obter informação adicional que melhore a avaliação de risco existente;

c) Analisar eventos ou ocorrências passadas;

d) Detetar alterações no contexto interno e externo, incluindo modificações no critério de risco e no próprio risco, que possam requerer uma revisão das medidas de controlo;

e) Identificar riscos emergentes;

f) Detetar e comunicar os resultados.

2.5.3 Tipologias

Avaliação contínua – avaliação contínua da eficácia dos controlos por parte do responsável do processo (em última análise responsável pela UO), permitindo identificar em tempo real e dando uma rápida resposta às insuficiências detetadas nos controlos existentes.

Nesta vertente, o responsável pelo processo deve manter um adequado nível de monitorização das atividades de controlo, de modo a manter disponível a seguinte informação:

- Descrição, caracterização e enquadramento do controlo do risco;

- Eventuais alterações introduzidas nas especificações do controlo (exemplo: alteração da periodicidade de execução);
- Evidências documentais (formato eletrónico, papel ou outro) da execução do controlo.

Esta informação deve encontrar-se disponível para o exercício da atividade de monitorização exercida de forma independente e será documentada em plataforma de SI específica para o efeito.

Avaliação independente ou separada – avaliação periódica da eficácia dos controlos pela auditoria interna e/ou por uma entidade independente. O âmbito e a frequência da avaliação independente ou separada é uma matéria de apreciação crítica pelos responsáveis destas áreas.

A avaliação independente ou separada deve ser exercida por uma área ou entidade que não esteja envolvida na conceção e implementação do controlo.

A avaliação independente ou separada revê, nomeadamente:

- O desenho dos controlos – revisão da adequação dos controlos ao propósito a que se destinam (especificações);
- A implementação dos controlos – verificação de que se encontram implementados de acordo com as especificações;
- A eficácia operacional dos controlos – revisão do funcionamento dos controlos, verificando se se encontram a mitigar o risco de acordo com o definido.

Sem prejuízo de outras obrigações de comunicação inerentes à realização de avaliações independentes, o responsável pelo controlo deve ser informado pela entidade que realize estas avaliações sobre:

- Âmbito da monitorização;
- Período previsto para a realização da monitorização;
- Resultados preliminares para efeitos do exercício de contraditório;
- Resultados finais da monitorização.

O responsável pelo processo objeto de avaliação independente assegura que as atividades de monitorização não afetam o normal desenrolar do processo, dando a sua anuência ou alertando para eventuais conflitos, os quais devem ser avaliados conjuntamente com a entidade que realiza a revisão independente.

A avaliação independente do controlo interno na Galp é realizada pelas seguintes áreas:

- Auditoria Interna, no âmbito das suas atribuições enquanto área responsável pela avaliação independente e sistemática das atividades da Galp através da revisão dos sistemas de gestão

de risco, da otimização dos processos de gestão, dos sistemas de controlo interno (incluindo o SCIRF) e de *governance*;

- Direção corporativa responsável pela segurança e sustentabilidade, no âmbito das suas atribuições enquanto área responsável pelas auditorias corporativas de AQS na Galp;
- Direção corporativa responsável pelos assuntos jurídicos e *governance,* no âmbito das suas atribuições de monitorização das políticas de controlo interno em matéria de *compliance* ético, regulatório e de *governance* da Galp.
- Auditores Externos, no âmbito das suas atribuições de certificação do SCIRF assim que o mesmo se encontre implementado.

2.6 Revisão e atualização do controlo interno

A revisão e atualização do controlo interno deve ocorrer, pelo menos, sempre que se verifiquem alterações relevantes ao nível dos processos relativos ao controlo interno, dos riscos, da atividade de controlo, dos aspetos regulatórios, dos sistemas de informação ou da estrutura organizativa da Galp, assim como ao nível das sociedades participadas, dos riscos de distorção material sobre o relato financeiro, e das recomendações da auditoria interna e externa.

Alguns exemplos de ocorrências que justificam a avaliação da necessidade de revisão e/ou atualização do controlo interno são:

- Alteração dos objetivos estratégicos da Galp;
- Mudanças relevantes na estrutura organizativa da Galp;
- Mudança de posicionamento da Galp;
- Admissão de novos colaboradores para posições chave na estrutura organizativa;
- Substituição ou implementação de um novo sistema de informação;
- Nova legislação / normativo interno;
- Criação de novas fontes de receita, através da introdução de novos produtos ou serviços; e
- Alteração dos processos e controlos existentes ou introdução de novos processos e controlos.

As atividades de revisão e atualização do controlo interno da Galp devem avaliar (i) a persistência do risco, (ii) a existência de novos riscos, (iii) o impacto e a probabilidade dos riscos que se tenham alterado, (iv) a eficácia dos controlos internos, e (v) a necessidade de redefinir os controlos e a sua periodicidade, devendo resultar no estabelecimento de mecanismos de gestão para os novos controlos.

3. Requisitos específicos

Devido ao impacto significativo na organização e à relevância e ao destaque que o modelo de referência COSO - *Internal Control Integrated Framework* atribui ao (i) reporte de informação financeira e não financeira, (ii) à prevenção da fraude, (iii) à segregação de funções, e (iv) à utilização de prestadores de serviços e de tecnologias de suporte às atividades, são estabelecidos neste capítulo do Manual requisitos específicos aplicáveis em relação a estas matérias.

3.1 Preparação e reporte de informação financeira e não financeira

3.1.1 Aspetos gerais

A conceção, implementação e funcionamento das atividades de controlo no domínio da preparação e divulgação de informação financeira e não financeira devem observar requisitos específicos em face do relevo da sua divulgação e do seu impacto na tomada de decisão de acionistas, investidores e outros *stakeholders*.

Os principais objetivos relacionados com a preparação e divulgação de informação financeira e não financeira são:

- O cumprimento de normas e regulamentação aplicável, incluindo o que diz respeito ao domínio contabilístico e de mercado de capitais;
- O adequado reporte dos eventos, transações e operações da Galp em conformidade com o referencial contabilístico aplicável;
- O adequado reporte aos seus *stakeholders* dos aspetos materiais de ESG.

A necessidade da Galp efetuar apreciações críticas, em particular em mensurações subjetivas que contêm estimativas e pressupostos, em eventos ou transações complexas para a preparação de divulgações de forma fiável e transparente, é inerente à informação financeira e à aplicação das políticas contabilísticas utilizadas na preparação das demonstrações financeiras.

Periodicamente são atualizados os princípios contabilísticos decorrentes de alterações estabelecidas em normas e regulamentação aplicável.

O principal risco associado ao reporte de informação financeira e não financeira consiste na omissão material ou em erros na preparação e/ou divulgação de informação. A materialidade dos eventos expressos nas demonstrações financeiras define o montante limite para determinar se um montante financeiro assume relevância.

Um dos requisitos fundamentais aplicáveis à Galp enquanto sociedade cotada consiste na apresentação ao mercado de um relato financeiro fiável e livre de omissões ou distorções materiais. Por forma a atingir este objetivo, a Galp identifica e intervém sobre os riscos que, individualmente ou em combinação, possam resultar em omissões ou distorções materiais das demonstrações financeiras, resultantes de erros ou fraude.

Em particular no que respeita à fraude, são consideradas as áreas de relato financeiro externo fraudulento e a apropriação indevida de ativos em quatro pontos de foco: 1) as tipologias de fraude possíveis, 2) a avaliação dos incentivos e pressões, e 3) a avaliação das oportunidades, sempre tendo presente a probabilidade de incidência e a magnitude de impacto.

Os riscos de omissão ou distorção material nas demonstrações financeiras são mitigados por atividades de controlo relevantes para relato financeiro, que respondem a asserções sobre a informação contida nas demonstrações financeiras. A Galp seleciona, desenvolve e aplica controlos que afetam os princípios de cada componente das suas demonstrações financeiras e que respondem a cada risco avaliado. É efetuada apreciação crítica no desenvolvimento das respostas adequadas para mitigar os riscos de omissão ou distorção material das demonstrações financeiras, considerando entre outros, a materialidade sobre as demonstrações financeiras, as áreas de negócio nas quais a Galp opera, os mercados geográficos, a dependência tecnológica, o âmbito e natureza do modelo de governo e as normas e regulamentos aplicáveis.

3.1.2 Princípios e asserções sobre o reporte de informação financeira e não financeira

As seguintes asserções são consideradas no reconhecimento, mensuração, apresentação e divulgação de rubricas, transações e eventos incluídos nas demonstrações financeiras consolidadas da Galp:

- Existência ou ocorrência – as transações registadas correspondem a eventos que ocorreram num determinado período;
- Plenitude – todas as transações e outros eventos ou circunstâncias que ocorreram num determinado período e que devem ser reconhecidas nesse período, encontram-se registadas;
- Exatidão – valores e outros dados relacionados com as transações ou eventos encontram-se apropriadamente registados;
- Corte de operações – as transações ou eventos são reconhecidos e registados no período em que ocorreram;
- Apresentação de divulgação – a informação encontra-se devidamente colocada, ordenada e classificada;
- Tempestividade (oportunidade) – a informação é apresentada atempadamente para a devida tomada de decisão dos *stakeholders*.

A preparação e apresentação de informação financeira tem ainda em consideração as seguintes asserções específicas:

- Direitos e obrigações – os direitos e obrigações são reconhecidos e registados no ativo e no passivo, respetivamente, num determinado momento;
- Valorização e classificação – os ativos, responsabilidades, transações, receitas e despesas são agregados e registados nos valores corretos no sistema contabilístico em conformidade com os princípios contabilísticos relevantes;

A preparação e apresentação de informação financeira e não financeira tem ainda em consideração os seguintes princípios específicos:

- Equilíbrio – A informação reflete o desempenho da organização de forma imparcial, apresentando aspetos positivos e negativos que permitam uma avaliação equilibrada do seu desempenho;
- Comparabilidade – A informação é consistente de modo a permitir aos *stakeholders* analisar alterações ao longo do tempo e comparar com outras organizações similares; e
- Clareza – A informação é apresentada de forma compreensível e acessível para os *stakeholders*.

3.1.3 Abordagem ao risco na preparação e divulgação de informação financeira ao mercado de capitais

Atendendo aos principais objetivos e princípios elencados acima, a preparação e divulgação de informação financeira, para fins de relato de informação financeira deve ser efetuada de acordo com a seguinte abordagem:

- Avaliação e determinação da materialidade das divulgações e rubricas, mediante fatores quantitativos e qualitativos;
- Identificação das divulgações e rubricas relevantes das demonstrações financeiras, baseada em fatores de risco de distorção material e incluindo considerações de materialidade;
- Identificação das asserções relevantes para cada uma dessas rubricas e divulgações, incluindo as transações e eventos subjacentes, bem como os processos que as suportam;
- Revisão periódica da consistência das políticas contabilísticas da Galp face aos princípios contabilísticos;
- Para as asserções relevantes das demonstrações financeiras, ao nível de cada rubrica e divulgação relevante, deve proceder-se à identificação de riscos de distorção nas demonstrações financeiras, atendendo a fatores qualitativos de risco e a critérios de probabilidade desses riscos. Esta abordagem deve ser aplicada aos processos de negócio, às unidades de negócio, e a um nível mais granular, às sociedades participadas que suportam as

rubricas das demonstrações financeiras e as divulgações definidas como materiais. O processo de identificação deve envolver o levantamento e a discussão com o responsável de cada um destes processos de negócio, destas unidades de negócio e destas sociedades participadas;

- Avaliação dos riscos de fraude e identificação das abordagens e circunstâncias em que podem ocorrer.

3.1.4 Controlo interno na preparação e divulgação de informação financeira ao mercado de capitais

O sistema de controlo interno na preparação e divulgação de informação financeira ao mercado de capitais deve ser desenhado e funcionar de forma integrada com a abordagem ao risco descrita no ponto 3.1.3 deste Manual.

A integração assegura uma resposta ao risco ao nível das asserções relevantes das demonstrações financeiras e deve ocorrer através da seleção e mapeamento de atividades de controlo que mitigam cada risco identificado.

O processo de seleção e implementação das atividades de controlo, tipicamente inclui os seguintes métodos e abordagens:

- Envolvimento dos responsáveis pela identificação das atividades de controlo, incluindo os responsáveis pelos processos de negócio e UO, os responsáveis da função financeira e os responsáveis pelos sistemas de informação que suportam os processos de negócio relevantes, entre outros;
- Utilização de matrizes para mapeamento das atividades de controlo aos riscos identificados, quer ao nível dos processos de negócio quer ao nível dos sistemas de informação;
- Realização de *workshops* para identificação de atividades de controlo apropriadas para cada risco;
- Utilização de *walkthroughs* para entender os processos de negócio, os controlos existentes, bem como os sistemas de informação e suas interdependências;
- Utilização de exemplos de atividades de controlo de acordo com boas práticas, devidamente customizadas;
- Avaliação das atividades de controlo existentes nos prestadores de serviços ou implementação de atividades de controlo sobre as atividades desenvolvidas ou informação

processada pelos mesmos, quando impacte as demonstrações financeiras, bem como dos seus sistemas de informação de suporte;

- Consideração das atividades de controlo automáticas existentes, bem como a avaliação da possibilidade de seu uso, atendendo ao ambiente dos sistemas de informação em que se inserem, e a consideração de atividades de controlo manuais;

- Utilização de uma combinação das atividades de controlo preventivas e detetivas, que melhor respondam aos fatores de risco;

- Identificação de funções incompatíveis e sempre que existam constrangimentos que impossibilitem uma adequada segregação de funções, devendo ser consideradas atividades de controlo de revisão a um nível de detalhe que permita a identificação de erros.

As atividades de controlo para o reporte de informação financeira e não financeira devem seguir os princípios apresentados neste capítulo, bem como os requisitos específicos de prevenção da fraude, segregação de funções, contratação de prestadores de serviços e utilização de tecnologias de suporte.

O controlo interno sobre a preparação e reporte de informação financeira e não financeira apresenta ainda as seguintes especificidades:

- **Identificação, conceção e implementação de atividades de controlo** – As áreas processuais que contribuem para a preparação e divulgação de informação financeira e não financeira devem constar do Modelo de Processos da Galp. Adicionalmente, na identificação, conceção e implementação de atividades de controlo são considerados os principais riscos na preparação da informação financeira e não financeira, sendo as atividades de controlo caracterizadas quanto às asserções a que dão resposta.

- **Prestadores de serviços relevantes para o reporte de informação financeira** – sem prejuízo dos requisitos específicos para prestadores de serviços estabelecidos no capítulo 3.4 deste Manual, a contratação de prestadores de serviços cujas atividades desenvolvidas ou informação processada possua impacto nas demonstrações financeiras da Galp deve considerar a avaliação dos seguintes aspetos:

    - Risco de omissão material ou de erros na preparação e divulgação de informação financeira, incluindo os relacionados com o manuseamento de ativos suscetíveis de perda ou apropriação indevida;

- A interdependência entre as atividades/tarefas e as atividades de controlo realizadas pelo prestador de serviço e aquelas realizadas pela Galp;
- Atividades de controlo realizadas pelo prestador de serviço relevantes para o reporte de informação financeira. Neste âmbito deve ser obtido do prestador de serviço, sempre que possível, um relatório independente sobre a conceção, implementação e eficácia das atividades de controlo[1];
- Atividades de controlo realizadas pela Galp de monitorização e supervisão das atividades de controlo realizadas pelo prestador de serviço.

- **Tecnologias de suporte ao reporte de informação financeira e não financeira** – A aplicação dos requisitos específicos relacionados com tecnologias de suporte previstos no capítulo 3.5. deste Manual no contexto do reporte de informação financeira e não financeira assume uma especial relevância na Galp devido à forte dependência tecnológica das respetivas áreas processuais.

  Reconhecendo esta dependência, a Galp caracteriza as atividades de controlo para o reporte de informação financeira e não financeira quanto à utilização de tecnologias de suporte (aplicação/sistema de informação) e identifica as atividades de controlo sobre essas tecnologias.

  A Galp reconhece ainda o papel da utilização de *software* de produtividade, nomeadamente aplicações de folhas de cálculo e de bases de dados, no suporte das atividades e controlos relevantes para o reporte de informação financeira e não financeira, avaliando os riscos subjacentes e identificando atividades de controlo de validação, monitorização e supervisão sobre a utilização das referidas aplicações.

  As atividades de controlo sobre tecnologias de suporte realizadas por prestadores de serviços devem ser incluídas, sempre que tal possa ser disponibilizado, num relatório independente sobre a conceção, implementação e eficácia das atividades de controlo.

- **Contexto normativo** – A Galp prepara as suas contas em conformidade com as normas internacionais de contabilidade IFRS, aprovadas pela União Europeia. Para colmatar situações de inexistência ou insuficiência nos normativos IAS/IFRS ou interpretações SIC/IFRIC, a Galp tem normas e procedimentos preparados com base nas melhores práticas de mercado e que aplica internamente em complemento das normas IFRS.

[1] "*Assurance Reports on Controls at a Service Organization*" de acordo com norma adequada (e.g. ISAE3402, SSAE16)

A Galp reporta o seu desempenho não financeiro no Relatório de Gestão e Contas, de acordo com os requisitos e diretrizes da *Global Reporting Initiative standards* e as diretrizes para o reporte integrado do *International Integrated Reporting Council*, entre outras referências internacionalmente reconhecidas.

Este reporte é efetuado em alinhamento com os requisitos de divulgação de informação não financeira requeridos pela Diretiva 2014/95/UE do Parlamento Europeu e do Conselho, de 22 de outubro de 2014, transposta pelo Decreto-Lei n.º 89/2017, de 8 de julho no que se refere à divulgação de informações não financeiras, incluindo informações sobre diversidade.

A Galp reporta ainda no seu Relatório de Gestão e Contas o sistema e as práticas de governo da sociedade, nos termos da regulamentação aplicável.

3.1.5 Informação e comunicação

O processo de divulgação de informação financeira e não financeira obrigatória deve ser acompanhado tanto pelos órgãos de administração e fiscalização como pelas UO.

Os documentos de apresentação de informação financeira e não financeira ao mercado de capitais são elaborados pela área responsável pelas relações com investidores, com base na informação disponibilizada pelas áreas responsáveis pelo planeamento e controlo das unidades de negócio, pela área responsável pela contabilidade, pela área responsável pelo planeamento e controlo corporativo e pelas áreas corporativas responsáveis pela sustentabilidade e pelo *governance*, conforme atribuições previstas em norma orgânica.

Em particular, relativamente à prestação de contas anuais e semestrais, os documentos são enviados aos órgãos de administração e de fiscalização, que procedem à sua aprovação antes de serem divulgados.

3.2 Prevenção de fraude

Um dos pontos de foco da componente de avaliação de risco do sistema de controlo interno é a identificação e avaliação dos riscos de fraude, assim como a identificação de falhas existentes ao nível do ambiente de controlo e das atividades de controlo que potenciem situações de fraude.

Os intervenientes no sistema devem criar controlos de prevenção de fraude que considerem os seguintes aspetos:

- Grau das estimativas na divulgação de informação;
- Esquemas de fraude comuns no setor e mercado da indústria;

- Regiões geográficas onde a Galp opera;
- Incentivos que possam motivar comportamentos fraudulentos;
- Natureza da tecnologia utilizada e capacidade de manipulação da informação;
- Complexidade das transações relevantes ou transações incomuns sujeitas a influência da gestão;
- Vulnerabilidade do sistema de controlo interno à sobreposição da gestão e/ou atuações que possam contornar as atividades de controlo existentes.

As situações de fraude a prevenir apresentam-se tipicamente da seguinte forma:

- Relato financeiro ou não financeiro fraudulento – Atos realizados com a intenção de iludir os utilizadores dos reportes financeiros ou não financeiros e que podem resultar em omissões significativas ou distorção da informação desses relatórios ou ainda num nível de precisão inferior à pretendida;
- Apropriação indevida de ativos – Apropriação de ativos da Galp, podendo resultar em omissões significativas ou distorção da informação dos relatórios externos financeiros;
- Atos ilegais – Violação de leis ou regulamentos com impacto direto ou indireto nos relatórios financeiros e não financeiros.

Os intervenientes no controlo interno devem ainda considerar os três principais fatores que estão na origem dos atos fraudulentos:

1. Incentivos ou pressões – existência de pressões excessivas para o cumprimento de objetivos ou obrigações, profissionais ou pessoais.

Apenas a título ilustrativo, alguns exemplos de situações que podem estar na origem da divulgação fraudulenta de informação são:

- ameaça à estabilidade financeira ou rentabilidade por alterações na economia, indústria ou condições de operação;
- pressão excessiva ao nível dos órgãos sociais para alcançar exigências ou expectativas dos *stakeholders*;
- existência de informação que denote ameaças à situação financeira de pessoas chave na Empresa, que sejam consequência do desempenho financeiro da Empresa;
- pressão excessiva sobre colaboradores para o cumprimento de objetivos.

Apenas a título ilustrativo, alguns exemplos de situações que podem estar na origem da apropriação indevida de ativos são:

- compromissos ou obrigações pessoais que criem pressão sobre colaboradores com acesso a dinheiro ou outros ativos suscetíveis de serem furtados;

- deterioração do relacionamento entre a Empresa e colaboradores com acesso a dinheiro ou outros ativos suscetíveis de serem furtados.

2. Oportunidade – existência de circunstâncias que favorecem atos de fraude, as quais se encontram na origem do método pelo qual a fraude é cometida.

Apenas a título ilustrativo, alguns exemplos de situações que podem estar na origem da divulgação fraudulenta de informação são:

- ineficácia ou inexistência de supervisão da atividade da Administração;
- estrutura organizacional complexa ou instável;
- deficiências no controlo interno resultantes de insuficiente supervisão, elevada rotação de pessoal em áreas relevantes para o reporte de informação financeira ou insuficiências nos sistemas de informação.

Apenas a título ilustrativo, alguns exemplos de situações que podem estar na origem da apropriação indevida de ativos são:

- manuseamento de elevados volumes de dinheiro, outros valores ou ativos facilmente convertíveis em dinheiro;
- manuseamento de artigos de inventário (matérias primas ou produto acabado) de reduzido tamanho e elevado valor;
- inexistência de uma adequada segregação de funções.

3. Racionalização – autojustificação por parte de quem comete fraude, tornando-a assim aceitável do seu ponto de vista.

A título ilustrativo, alguns exemplos de situações que podem estar na origem de divulgação fraudulenta de informação são:

- falhas ou ineficácia na comunicação dos valores da organização;
- excessivo envolvimento de gestores de áreas não financeiras em matérias financeiras;
- justificação ou tentativa de justificação sucessiva de erros contabilísticos com base na materialidade.

A título ilustrativo, alguns exemplos de situações que podem estar na origem da apropriação indevida de ativos são:

- subvalorização da necessidade de monitorizar riscos relacionados com a apropriação indevida de ativos;
- subvalorização dos controlos sobre apropriação indevida de ativos, não cumprindo os controlos definidos ou não tomando as medidas de correção em deficiências conhecidas;

- comportamentos que indiciem desconsideração para com a Empresa ou a sua forma de tratar os colaboradores;
- alterações nos comportamentos ou estilo de vida.

O controlo interno assume um papel fundamental na prevenção e deteção de fraude, eliminando ou mitigando as causas que estão na sua origem, o qual é demonstrado da seguinte forma:

a) Ambiente de Controlo – A prevenção da fraude é considerada no Código de Ética e Conduta da Galp e no canal de comunicação de irregularidades (disponível no site oficial da Galp e na intranet neste link);

b) Avaliação de risco – São realizadas pela segunda linha de defesa análises de risco direcionadas ao risco de fraude, as quais são consideradas na elaboração de programas de auditoria interna presentes na terceira linha de defesa;

c) Atividades de controlo – Devem ser concebidas e implementadas atividades de controlo direcionadas para a mitigação do risco de fraude, nomeadamente através de:

- Segregação de funções, melhor descrito no capítulo 3.3 deste Manual;
- Supervisão das funções responsáveis por manipulação e gestão de dinheiro ou ativos suscetíveis de fraude (ao nível da área corporativa responsável pela tesouraria e finanças corporativas);
- Desenho, implementação e execução de atividades de controlo que mitiguem o risco de fraude, ao nível dos processos de negócio nos quais se possa manifestar com um impacto relevante nas rubricas das demonstrações financeiras, ou de forma pervasiva ao nível das demonstrações financeiras como um todo;
- Regras e procedimentos internos para aprovação de transações nas áreas processuais de despesa e receita, bem como de transações relevantes, complexas ou não usuais;
- Regras e procedimentos para custódia de ativos suscetíveis de fraude;
- Reconciliações incidindo sobre ativos suscetíveis de fraude;
- Procedimentos de manutenção de informação documentada sobre estimativas contabilísticas, sobre transações relevantes, complexas ou não usuais e sobre lançamentos contabilísticos manuais, e atividades de controlo de revisão, autorização e aprovação das mesmas;
- Rotação de colaboradores em funções suscetíveis de fraude;
- Verificação dos antecedentes de candidatos para funções mais suscetíveis para o cometimento de fraude, no âmbito dos processos de recrutamento e mobilidade da Galp;

- Restrição de acessos nos sistemas de informação de acordo com as funções e responsabilidades.

a) Informação e comunicação – existência de canal para comunicação de irregularidades (opentalk@galp.com) com vista à averiguação dos factos e definição atempada das medidas apropriadas;

b) Atividades de monitorização – Supervisão pela terceira linha de defesa do funcionamento do controlo interno no que diz respeito ao risco de fraude.

3.3. Segregação de funções

3.3.1 Objetivos

Durante o processo de definição e implementação de atividades de controlo deve ser assegurada uma adequada segregação de funções, em particular nas transações que representam um maior risco para o negócio.

Na medida em que permitem gerir e monitorizar as funções que devem ser segregadas, a utilização de tecnologias de informação deve ser sempre considerada, realizando-se uma análise de custo/benefício quanto à sua utilização.

A segregação de funções visa contribuir para:

- *Compliance* regulatória – Quando é exigida por lei ou por entidades reguladoras;
- Segurança e gestão de dados – Quando é necessária para a proteção da privacidade e/ou para a prevenção de violações de segurança;
- Mitigação do risco de omissão material ou erros no reporte de informação financeira;
- Prevenção da fraude – Enquanto controlo primordial para prevenir a realização de ações fraudulentas resultantes de acumulação indevida de funções;
- Supervisão e revisão de atividades de controlo;
- Deteção atempada de erros que possam ocorrer;
- Alinhamento entre os processos de negócio e os controlos nos sistemas de informação da Galp.

Os intervenientes no sistema de controlo interno devem:

1. Definir as regras de segregação de funções, tendo em consideração, nomeadamente, a necessidade de uma correta gestão de acessos;
2. Identificar as funções que devem ser segregadas nos processos relevantes;
3. Assegurar o alinhamento prévio da decisão sobre as funções que devem ser segregadas com os responsáveis dos processos;

4. Definir controlos de mitigação que deem resposta a funções que não são possíveis de segregar (controlos compensatórios);
5. Efetuar avaliações periódicas à adesão por parte de todos/as os/as colaboradores/as da Galp às normas e regras aplicáveis.

A segregação de funções na Galp baseia-se no princípio de limitação da acumulação de funções ao longo das várias fases de um mesmo processo, nomeadamente que envolvam responsabilidades distintas sobre cada uma das seguintes tarefas:

- Executante;
- Aprovador;
- Revisor / supervisor.

3.3.2 Principais exemplos de conflitos na preparação e divulgação de informação financeira

No que respeita à preparação e divulgação de informação financeira, e de acordo com as melhores práticas, a segregação de funções deve, pelo menos, considerar os seguintes principais conflitos, a fim de minimizar o potencial de encobrimento de fraude, ocultação de erros, desvio de ativos e/ou ocultação da sua apropriação indevida:

- Verificar, autorizar ou aprovar pagamentos conflitua com a respetiva preparação;
- Verificar/retificar, autorizar ou assinar pagamentos conflitua com a edição de dados mestre de fornecedores;
- Autorizar compras de imobilizado conflitua com a edição de dados mestre de imobilizado;
- Autorizar inventário ou despesas com compras conflitua com a edição de dados mestre de inventário;
- Editar dados mestre de registo de remunerações conflitua com a aprovação do processamento ou a autorização do pagamento de remunerações;
- Editar os dados mestre de contas a receber conflitua com o acesso a fundos/dinheiro;
- Iniciar transações de investimento, de derivados ou de crédito conflitua com o registo das respetivas transações;
- Reconciliar contas conflitua com a preparação de depósitos;
- Produzir auditorias internas ou relatórios financeiros conflitua com a revisão e aprovação de demonstrações financeiras.

3.3.3 Controlos Compensatórios

Caso não seja possível ou viável assegurar uma adequada segregação de funções, particularmente devido à inexistência de recursos suficientes, ou limitação dos sistemas de informação em espelhar a segregação de funções nas respetivas permissões de acesso, devem ser implementados controlos compensatórios.

Algumas atividades, devido à sua criticidade, podem justificar a existência de medidas de mitigação adicional do risco, como por exemplo as atividades que envolvem o manuseamento direto de dinheiro, contas bancárias ou outros ativos de elevado valor.

Nestas circunstâncias devem ser identificados controlos compensatórios ou formas alternativas de mitigação do risco.

A título ilustrativo, alguns exemplos de controlos compensatórios preventivos são:

- Dupla autorização – a autorização/aprovação exige a intervenção de dois intervenientes. Exemplo: duas assinaturas para autorização de movimentos bancários;
- Restrição física – existência de restrições de acesso físico que impeçam a concretização do risco. Exemplo: controlo de acessos a zonas de movimentação de mercadorias de armazéns.

A título ilustrativo, alguns exemplos de controlos compensatórios detetivos são:

- Revisão independente – revisão independente das operações (pela totalidade das operações ou com base numa amostra) sujeita a restrições de segregação de funções. Exemplo: revisão mensal das ordens de compra registadas;
- Alerta automático – alertas que são emitidos mediante determinadas circunstâncias cumulativas de risco. Exemplo: colocação de ordens de compra e receção de mercadoria para compras de valor superior a um determinado valor;
- Relatório de exceções – relatórios que sistematizam as operações onde foram violados os princípios de segregação de funções, os quais devem ser analisados e validados. Exemplo: lista de alterações a dados mestre de fornecedores.

3.4 Prestadores de serviços

Previamente à decisão de contratar terceiros para a execução de processos ou controlos da responsabilidade da Galp, os intervenientes no sistema de controlo interno devem identificar e avaliar os riscos específicos que essa decisão pode acarretar para a Galp.

A gestão do sistema de avaliação e qualificação dos fornecedores da Galp é realizada pela área corporativa responsável pelas aquisições de bens e serviços da Galp nos termos da norma interna que regula o processo de compras (disponível na intranet da Galp neste link), bem como pelas normas internas procedimentais sobre a integração de requisitos AQS (disponível na intranet da Galp

neste link) e de requisitos de privacidade e cibersegurança no processo de contratação de fornecedores (disponível na intranet da Galp neste link).

Para determinar as ações que devem ser implementadas para mitigar os riscos identificados, deve ser definida a significância dos serviços prestados por terceiros, tendo em conta os seguintes critérios:

- Relevância das transações e/ou informação processada para os objetivos operacionais, de reporte e de conformidade da Galp;
- Natureza e complexidade dos serviços prestados e o respetivo nível de normalização;
- Grau de responsabilidade concedido ao prestador de serviços através dos termos contratuais; e
- Impacto sancionatório associado ao incumprimento da atividade quando esta seja uma imposição legal ou regulamentar.

A Galp utiliza nos contratos estabelecidos com os prestadores de serviços preparados pela área corporativa responsável pelos assuntos jurídicos elementos que acautelam os requisitos acima referidos.

A conceção, implementação e funcionamento dos controlos a implementar para mitigar os riscos identificados neste capítulo é da responsabilidade da área corporativa de compras ou área equivalente nas UO, quanto aos processos de compra que não se encontram sob a responsabilidade daquela, em articulação com as áreas corporativas responsáveis pelos assuntos jurídicos e *governance* e gestão de risco.

3.5 Tecnologias de suporte

A utilização de tecnologia pela Galp requer a conceção e implementação de controlos que mitiguem os riscos específicos associados e assegurem o devido funcionamento dos processos, respetivas normas, procedimentos ou atividades de controlo, aos quais essa tecnologia dá suporte.

As tecnologias de suporte devem ser utilizadas de acordo com o estabelecido em normas e procedimentos.

De forma não exaustiva, as tecnologias de suporte incluem os seguintes elementos, aos quais estão associados riscos específicos:

a) Infraestrutura tecnológica e operações – riscos no funcionamento das tecnologias de suporte, as quais dependem de infraestruturas, próprias ou contratadas a terceiros, de recursos computacionais (exemplo: servidores), de comunicações ou de energia. Devem ser considerados os riscos relacionados com interdependências existentes entre as tecnologias de

suporte, nomeadamente ao nível da transferência de informação através de interfaces (automáticos ou manuais);

Os contratos em vigor de serviços de comunicações fixas, móveis, serviços de *midrange* (operação, manutenção e gestão dos servidores da Galp, bem como dos sistemas operativos e das bases de dados que suportam as várias aplicações) e de *datacenter* (alojamento dos servidores da Galp/*hosting*) definem obrigações dos fornecedores e regras de prestação do serviço (incluindo SLAs e penalidades) que mitigam adequadamente os riscos relacionados com infraestrutura tecnológica e operações.

b) Segurança – riscos de segurança das tecnologias de suporte e da informação por elas tratada, nomeadamente falhas e acessos ou uso indevidos, não autorizados ou contrários aos objetivos definidos pela Galp, de proveniência interna ou externa, incluindo riscos de Cibersegurança, à Galp. Adicionalmente, devem ser considerados riscos de segurança lógica e de segurança física.

   Os riscos de segurança encontram-se geridos na Galp com base na norma de gestão de segurança de informação. Os contratos de *datacenter*, contratos de comunicações fixas e móveis em vigor na Galp contribuem igualmente para a gestão dos referidos riscos.

c) Ciclo de vida das tecnologias de informação e comunicação – riscos com impacto no funcionamento dos processos, associados à identificação de necessidades do negócio, adoção ou aquisição, desenvolvimento, manutenção e descontinuação das tecnologias de suporte e respetiva infraestrutura tecnológica. A gestão deste ciclo de vida deve também assegurar um alinhamento das tecnologias utilizadas com os objetivos definidos pela Galp.

   A norma interna que regula as iniciativas e projetos de sistemas de informação da Galp e a norma setorial de arquitetura de informação da Galp que estabelece as arquiteturas de integração de dados entre aplicações (internas e externas) a implementar dão corpo na Galp à preocupação com este tema. Por outro lado, a Galp utiliza "Guias de Gestão de Projetos de SI" (link) que orientam e normalizam as práticas a seguir pelos gestores de projetos de sistemas de informação no desenvolvimento de projetos.

d) Prestadores de serviços – riscos específicos da prestação de serviços sobre tecnologias de suporte, complementando ou substituindo controlos que incidem sobre os aspetos referidos nas alíneas anteriores.

Em complemento, para efeitos do SCIRF deve ser mantido um ambiente de controlo sobre os sistemas de informação que suportam os processos de negócio e UO relevantes para as divulgações e as rubricas das demonstrações financeiras e seus interfaces, seguindo uma abordagem de

mapeamento dos riscos associados a sistemas de informação e aos Controlos Gerais Informáticos (CGI) que os visam mitigar, a descrever em Matrizes de Riscos e Controlos para Sistemas de Informação a adotar no âmbito do projeto de implementação do SCIRF.

Para reforçar a verificação do cumprimento dos requisitos dos projetos realizados pelos seus fornecedores e *outsourcers* de sistemas de informação, a Galp pode recorrer a serviços prestados por terceiros (i.e. de fornecedores distintos dos que estão a realizar os referidos projetos) para realizar testes adicionais e para apoiar/ complementar a realização de testes de aceitação, que são da responsabilidade das UO da Galp.

A extensão, tipologia e grau de automatização dos CGI deve atender à complexidade das tecnologias envolvidas, dos riscos a que se encontram expostas, da utilização de prestadores de serviços e dos riscos associados aos processos a que dão suporte.

A conceção dos CGI, com base nos requisitos de negócio definidos pelas UO, a sua implementação no sistema e a garantia do seu funcionamento são da responsabilidade da área corporativa de IT & Digital.

Estas áreas colaboram com a área funcional de segurança e sustentabilidade dno que diz respeito à segurança física das tecnologias de suporte.

É ainda responsabilidade da área de IT & Digital e CISO (*Chief Information Security Officer*):

a) Identificar riscos específicos decorrentes da utilização de determinadas tecnologias ou de alterações introduzidas nas tecnologias de suporte ou infraestruturas tecnológicas de que dependam, no pressuposto de que as opções tecnológicas sejam igualmente da sua responsabilidade; e

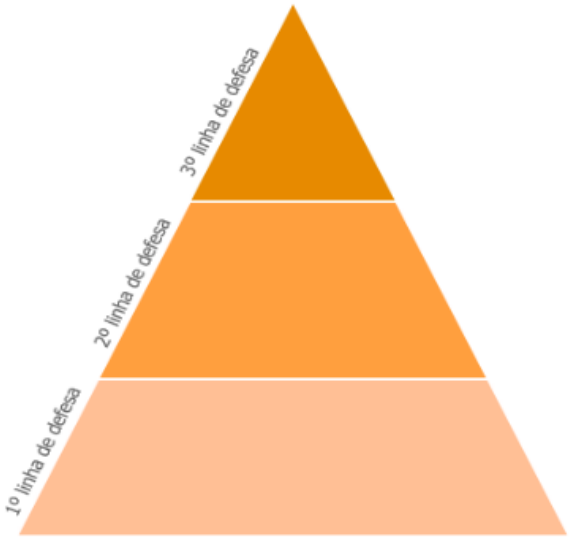
b) Definir os requisitos de informação a obter das UO necessários para a conceção, implementação e funcionamento dos CGI.

A norma interna relativa ao processo de registo de pedidos e incidentes SI (link), que define os passos necessários ao registo e tratamento de incidentes, assegura a obtenção de informação por parte das UO.

4. Modelo de Governo

4.1 As três linhas de defesa do controlo interno

O modelo de governo do controlo interno encontra-se estruturado de acordo com o princípio das três linhas de defesa.



A abordagem das três linhas de defesa possibilita um relacionamento consistente entre as atividades diárias de gestão do risco, a supervisão do risco ao nível dos processos do Grupo e a supervisão do risco estratégico e corporativo.

A constituição das linhas de defesa deve assegurar que as áreas funcionais e os seus intervenientes não acumulem funções em mais do que uma linha, exceto em caso de limitações de recursos ou organizacionais, situação na qual deverão ser assegurados controlos compensatórios.

Sem prejuízo da verificação do princípio disposto no parágrafo acima, algumas áreas organizacionais do centro corporativo acumulam responsabilidades em mais do que uma linha de defesa, nomeadamente:

- A área de IT & Digital desempenha essencialmente um papel de primeira linha de defesa ao ser responsável pela identificação e gestão dos riscos de sistemas e tecnologias de informação. Contudo, desempenha ainda um papel enquanto segunda linha de defesa pela responsabilidade de supervisão e monitorização dos riscos relacionados com os sistemas e tecnologias de suporte.

- A área de segurança e sustentabilidade desempenha essencialmente um papel de segunda linha de defesa pela responsabilidade de supervisão e monitorização dos riscos que lhe estão subjacentes. Contudo, desempenha ainda um papel de terceira linha de defesa pela sua responsabilidade na realização de auditorias independentes no âmbito da segurança e sustentabilidade;

- A acumulação de papéis enquanto segunda e terceira linhas de defesa também se verifica na área corporativa de assuntos jurídicos e *governance* no que respeita às auditorias de *compliance*.

A definição das três linhas de defesa está estabelecida no Modelo de Governo de Gestão de Risco, acessível neste (link)

5. Matriz de responsabilidades

	Auditor Externo/ROC	Conselho Fiscal	Conselho de Administração	Comissão Executiva	Unidades de negócio	Sistemas de Informação	Financeira	Operações de RH e recompensa	Compras	Comunicação externa	Relações com Investidores	Investigação e tecnologia	Engenharia e gestão de projetos	Relações laborais	Gestão do património	Seguros	Assuntos Jurídicos e resolução de conflitos	Sistemas de informação	Compliance e estratégia fiscal	Ambiente, qualidade, segurança e sustentabilidade	Governance e Compliance	Planeamento e controlo de gestão	Estratégia	Gestão de risco	Comissão de Gestão de Risco	Comissão de Sustentabilidade	Comissão AQS Corporativa	Comissão de Ética e Conduta	Ambiente, qualidade, segurança e sustentabilidade	Auditoria Interna	Governance e Compliance
					1ª Linha													2ª Linha												3ª Linha		
Ambiente de Controlo																															
Conceber e implementar controlos de alto nível		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C	I	I	I
Acompanhar e supervisionar o sistema de controlo interno	I	R	A	I																									C	C	C
Promover cultura organizacional e compromisso com o controlo interno		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C	I	I	I
Definir linhas de reporte, competências e responsabilidades do controlo interno		I	A	R	I	I	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C	I	I	I
Atribuir responsabilidades sobre o controlo interno		I	A	A	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Avaliação de Risco																															
Identificar e analisar riscos				A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Definição dos níveis de tolerância dos riscos			A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	C	C	C	C	C	C	C	C			
Avaliar riscos identificados					R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Monitorizar os riscos		I	A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R
Rever os riscos		I	A	A	R	R	R	R	R	R	R	R	R	R	R	R	R	I	I	I	I	I	I	I	I	I	I	I			
Acompanhar e supervisionar o sistema de gestão de riscos	I	R	R	C	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	I	C	I	I	I	C	C	C
Atividades de Controlo																															
Conceber controlos nos processos				A	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R			
Implementar controlos nos processos				A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	C	C	C	C	C	C	C	C			
Conceber controlos gerais informáticos				A	C	R	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C			
Implementar controlos gerais informáticos				A	I	R	I	I	I	I	I	I	I	I	I	I	I	C	C	C	C	C	C	C	C	C	C	C			
Executar atividades de controlo				A	R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	C	C	C	C	C	C	C	C			
Desenvolver atividades de controlo através de normas e procedimentos					R	R	R	R	R	R	R	R	R	R	R	R	R	C	C	C	A	C	C							I	
Informação e Comunicação																															
Identificar e comunicar insuficiências de informação relevante para o controlo interno		I		I	R	R	R	R	R	R	R	R	R	R	R	R	R	A	A	A	A	A	A	A	A	A	A	A	I	I	I
Monitorização																															
Monitorizar a eficácia dos controlos implementados (Monitorização interna)					R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R			
Avaliar a eficácia do controlo interno e dos respetivos procedimentos (Monitorização independente)	R	I	I	I	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	R	R	R
Rever e atualizar o controlo interno		I			R	R	R	R	R	R	R	R	R	R	R	R	R	A	A	A	A	A	A	A	A	A	A	A	I	I	I
Moinitorizar e acompanhar o desenvolvimento do controlo interno	I	I	I	I														C	C	C	C	C	C	C	C	C	C	C	R	R	R

R Responsável (Executante) A Aprovador C Consultado I Informado

6. Verificação periódica de adequabilidade

A Área de Controlo Interno e a Direção de Assuntos Jurídicos e *Governance* asseguram a monitorização periódica do presente Manual com vista a verificar a sua adequação ao cumprimento dos mais avançados padrões de controlo interno.

O presente Manual é periodicamente sujeito a verificação de adequabilidade, em prazo não superior a 3 anos.

7. Disposições finais e transitórias

A presente norma produz efeitos a partir da data da sua publicação.

Eventuais dúvidas quanto à aplicação da presente norma devem ser remetidas à área de Controlo Interno da Galp.