PRESIDÊNCIA DO CONSELHO DE MINISTROS

Gabinete Nacional de Segurança

MANUAL DE GESTÃO DO RISCO

ÍNDICE

1. Enquadramento

O Plano de Recuperação e Resiliência (doravante designado "*PRR*"), aprovado a 16 de junho de 2021 pela Comissão Europeia (doravante designado "CE"), estabelece que a sua implementação implica a tomada de medidas adequadas que assegurem a boa utilização dos fundos do Mecanismo de Recuperação e Resiliência, em cumprimento da legislação comunitária e nacional aplicável, em especial no que se refere à prevenção, deteção e correção de fraude, corrupção e conflito de interesses.

O Gabinete Nacional de Segurança (doravante designado "*GNS*") e o Centro Nacional de Cibersegurança (doravante designado "*CNCS*") enquanto Beneficiários, Diretos e Intermediários, do PRR, e em cumprimento da Orientação Técnica n.º 7/2021 (OT 7/2021) e da Orientação Técnica n.º 14/2023 (OT 14/2023) da Estrutura de Missão Recuperar Portugal (doravante designado "EMRP"), comprometeu-se a seguir as metodologias, procedimentos e instrumentos de trabalho da EMRP, no sentido de garantir mecanismos de prevenção que permitam reduzir a ocorrência de situações de corrupção, tendo por base um sistema de gestão e controlo robusto, associado a uma avaliação de risco de fraude proactiva, estruturada e orientada, de forma a assegurar o princípio da boa gestão e a salvaguardar os interesses financeiros da União.

No âmbito do sistema de controlo interno implementado no GNS/CNCS, foram desenvolvidos vários mecanismos de combate à corrupção e infrações conexas, havendo agora a obrigação contratual de desenvolver um Manual de Gestão do Risco, que inclui informação sobre a metodologia de avaliação de risco de fraude e de reporte das situações de fraude às instâncias adequadas.

Assim, o presente Manual de Gestão do Risco do GNS/CNCS assume-se como um instrumento integrante do sistema de controlo interno, que inclui informação sobre a metodologia de avaliação de risco de fraude e de reporte das situações de fraude às instâncias adequadas contribuindo para prevenir, detetar e reportar situações de irregularidades e fraude.

2. Âmbito e Objetivos

O presente Manual de Gestão do Risco aplica-se a todos os colaboradores do GNS/CNCS, independentemente da função desempenhada, posição hierárquica ou vínculo. Através deste Manual, o PRR estabelece que deve ser plasmada a metodologia aplicada pelo GNS/CNCS na gestão e avaliação do risco de fraude e outras irregularidades e que os conceitos e linhas estratégicas que devem ser identificados são os seguintes:

- Definição de irregularidade, fraude e corrupção;
- Orientações sobre os requisitos mínimos para medidas antifraude eficazes e proporcionais: política antifraude; prevenção; deteção, correção e reporte;

› Autoavaliação do risco de fraude; inclui o instrumento de avaliação do risco, composição e competências da equipa de autoavaliação, frequência da autoavaliação, atribuição de responsabilidades e a ferramenta de avaliação do risco de fraude.

Assim, o GNS/CNCS estabelece que o presente Manual tem como objetivos:

› Apresentação da metodologia de avaliação do risco de fraude;
› Identificação dos riscos de fraude relativamente a cada área de risco;
› Com base na identificação dos riscos, indicação das medidas a implementar para prevenir a sua ocorrência;
› Elaboração de um relatório anual de avaliação do risco de fraude;
› Reporte das situações de fraude às instâncias adequadas

3. Estrutura Organizacional

3.1 GNS

O Gabinete Nacional de Segurança (GNS) tem por missão garantir a segurança da Informação Classificada (IC) no âmbito nacional e das organizações internacionais de que Portugal é parte, e exercer a função de autoridade de credenciação de pessoas singulares ou coletivas para o acesso e manuseamento de IC, bem como a de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado — Infraestrutura de Chaves Públicas (SCEE) e de entidade credenciadora por força do disposto na lei que regula a disponibilização e a utilização das plataformas eletrónicas de contratação pública, conforme o disposto no n.º 1 do Art.º 2.º do Decreto-Lei n.º 136/2017 de 6 de novembro.

3.1.1 Atribuições e competências.

De acordo com o n.º 2 do Art.º 2.º do Decreto-Lei n.º 3/2012 de 16 de janeiro e alterações introduzidas pelas alíneas c), d), e), h), l), e m) do n.º 3 do Art.º 2.º do Decreto-Lei n.º 136/2017 de 6 de novembro, o GNS detém as seguintes atribuições:

› Garantir a articulação e a harmonização dos procedimentos relativos à segurança da IC em todos os serviços, organismos e entidades, públicos ou privados, onde seja administrada tal informação, designadamente e em especial, os da Administração Pública, das Forças Armadas e das Forças e Serviços de Segurança, bem como no âmbito das organizações, reuniões, programas, contratos, projetos e outras atividades internacionais em que Portugal participe;
› Assegurar, nos termos dos instrumentos de vinculação do Estado Português, a proteção e a salvaguarda da IC emanada das organizações internacionais de que Portugal faça parte ou das

respetivas estruturas internas, nomeadamente no âmbito da Organização do Tratado do Atlântico Norte (OTAN), da União Europeia (UE), Unidade Europeia de Cooperação Judiciária (EUROJUST) e da Agência Espacial Europeia (AEE), bem como de outros Estados com os quais tenham sido celebrados acordos de segurança;

- Exercer, em Portugal, os poderes públicos cometidos às autoridades nacionais de segurança, nomeadamente nas áreas da credenciação de segurança, segurança das comunicações, distribuição de IC e outras, nos termos das normas aprovadas pelas entidades internacionais competentes;
- Proceder ao registo, distribuição e controlo da IC, bem como de todos os procedimentos inerentes à sua administração, de índole nacional ou confiadas à responsabilidade do Estado Português, garantindo que o material de cifra é objeto de medidas específicas de segurança e administrado por canais diferenciados;
- Fiscalizar e inspecionar as entidades que detenham, a qualquer título e em qualquer suporte, IC sob responsabilidade portuguesa, dentro e fora do território nacional;
- Avaliar, acreditar e certificar a segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de IC e proceder à realização de limpezas eletrónicas;
- Promover o estudo, a investigação e a difusão das normas e procedimentos de segurança aplicáveis à proteção e salvaguarda da IC, propondo a doutrina a adotar por Portugal e a formação de pessoal especializado nesta área da segurança;
- Credenciar as pessoas singulares ou coletivas que pretendam exercer as atividades de comércio e indústria de bens e tecnologias militares, nos termos da lei que regula as condições de acesso e exercício das atividades de comércio e indústria de bens e tecnologias militares;
- Credenciar entidades públicas e privadas para o exercício de atividades industriais, tecnológicas e de investigação, quando tal seja exigido por disposição legal ou regulamentar;
- Exercer as competências de autoridade credenciadora e de fiscalização de entidades que atuem no âmbito do Sistema de Certificação Eletrónica do Estado (SCEE), bem como no quadro do regime jurídico dos documentos eletrónicos e da assinatura eletrónica;
- Atuar como autoridade responsável pela componente codificada do Sistema GALILEO, credenciar os pontos de contacto nacionais no âmbito da sua componente de segurança e efetuar a gestão de chaves de cifra aquando da respetiva operação;
- Exercer as competências de entidade credenciadora no âmbito da lei que regula a disponibilização e a utilização das plataformas eletrónicas de contratação pública;
- Exercer as demais atribuições que lhe sejam atribuídas por lei.

3.1.2 Organograma

De acordo o disposto no artigo 4.º do Decreto-Lei n.º 170/2007, de 3 de maio, e do artigo 5.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, a organização interna do GNS obedece ao modelo de estrutura matricial.

A estrutura orgânica do GNS abaixo indicada corresponde à estrutura informal atualmente existente, aguardando-se a aprovação da portaria que fixará o número máximo de chefes de equipas multidisciplinares que integram a estrutura do GNS.

〉 Inspeção e Auditoria

A equipa multidisciplinar de Inspeção e Auditoria (IA) tem por missão apoiar a Autoridade Nacional de Segurança, garantindo a fiscalização e inspeção das entidades que detenham informação classificada sob responsabilidade portuguesa, dentro e fora do território nacional, de modo a verificar e promover o cumprimento dos normativos, procedimentos e condições de segurança aplicáveis a esse tipo de informação. Adicionalmente, apoia a Direção do Gabinete Nacional de Segurança a avaliar, por meio de auditorias, a adequação, a eficácia e o cumprimento dos procedimentos de controlo internos do GNS/CNCS, assim como o cumprimento de legislação aplicável.

〉 Doutrina e Formação

A equipa multidisciplinar de Doutrina e Formação (DF) desenvolve um conjunto de atividades centradas na dinamização de competências que visam a salvaguarda da Informação Classificada (IC).

Compete ao DF promover o estudo, a investigação e difusão de normas e procedimentos de segurança de IC a nível nacional, contribuir e acompanhar a doutrina emanada pelas organizações internacionais de que Portugal faz parte, conduzir, negociações técnicas tendentes ao estabelecimento de Acordos Bilaterais e Multilaterais de Segurança para a troca e proteção mútua da IC, assegurar ações de formação que visam preparar organizações e pessoas que manuseiem IC.

〉 Gestão da Informação Classificada e Criptografia

A equipa multidisciplinar de Gestão da Informação Classificada e Criptografia (GICC) tem por missão apoiar a Autoridade Nacional de Segurança e Autoridade nacional de Distribuição garantindo que a gestão do ciclo de vida da Informação Classificada é executada de maneira harmoniosa por todos os órgãos de segurança em território nacional e onde se encontrem implantados no estrangeiro, cumprindo com o normativo legal nacional e com as normas e procedimentos da Organização do Tratado do Atlântico Norte (OTAN), da União Europeia e de outras organizações de que Portugal faça parte, e que a administração e distribuição de material criptográfico se efetue por canais diferenciados.

〉 Segurança Digital Tecnológica e de Infraestruturas

A equipa multidisciplinar de Segurança Digital, Tecnológica e de Infraestruturas (SDTI) tem por missão apoiar a Autoridade Nacional de Segurança na Certificação e Acreditação de produtos, equipamentos, serviços, sistemas e instalações que processam informação classificada, assim como, no apoio ao desenvolvimento de projetos e programas com especial foco para a segurança digital, tecnológica e do Espaço. Apoiar ainda o Diretor Geral do GNS na supervisão dos sistemas de identificação eletrónica, serviços de confiança, na gestão das listas nacionais de confiança e credenciação de plataformas eletrónicas de contratação pública. Integra as áreas de Segurança Tecnológica, Segurança das Infraestruturas, Segurança do Espaço, e os Serviços de Confiança.

〉 Credenciação

A equipa multidisciplinar de Credenciação (CRED) tem por missão principal apoiar a Autoridade Nacional de Segurança na atribuição, controlo, alteração e cancelamento das credenciações de segurança de pessoas singulares e coletivas, públicas ou privadas, ou de qualquer outro serviço ou organismo, onde seja administrada informação classificada ou que necessitem de desenvolver atividades especificas que, nos termos da lei, envolvam a administração dessa informação.

〉 Informática, Redes e Comunicações

A equipa multidisciplinar de Informática, Redes e Comunicações (IRC), em colaboração com o CNCS/DST no que diz respeito à Rede Corporativa, presta um conjunto de serviços internos de suporte ao funcionamento do CNCS e do GNS, nomeadamente ao nível da gestão da infraestrutura e sistemas, da prestação de serviços informáticos de apoio ao utilizador, da gestão e operação de um Security Operations Centre (SOC) e do apoio à produção de normativos técnicos.

〉 Administração e Logística

À equipa multidisciplinar de Administração e Logística (ADMLOG) incumbe a assegurar as atividades do GNS/CNCS no domínio dos recursos financeiros, materiais e de pessoal, designadamente a realização dos processos de aquisição, do aprovisionamento, da gestão dos transportes internos, da manutenção e conservação das instalações, das viagens e deslocações em serviço, e também as atividades relacionadas com a gestão financeira, orçamental e patrimonial, bem como a cobrança da receita, a elaboração da prestação de contas e o processamento de abonos variáveis e eventuais do pessoal que presta serviço no GNS/CNCS.

3.2 CNCS

Através da Resolução do Conselho de Ministros n.º 42/2012, de 13 de abril, foi criada a comissão instaladora que tem por objetivo a criação, instalação e operacionalização de um CNCS. A 6 de outubro de 2014 foi criado o CNCS, dentro do GNS, através do Decreto-Lei n.º 69/2014, de 9 de maio.

O CNCS desenvolve a sua missão com o objetivo de contribuir para uma utilização livre, confiável e segura do ciberespaço de interesse nacional. Atuando como coordenador operacional e autoridade nacional em matéria de cibersegurança junto das entidades do Estado, operadores de infraestruturas críticas nacionais, operadores de serviços essenciais e prestadores de serviços digitais, o CNCS transporta também a sua ação para a sociedade em geral.

3.2.1 Atribuições e competências

Nos termos do número 1 do artigo 2.º-A do Decreto-Lei n.º 3/2012 de 16 de janeiro, o CNCS detém as seguintes competências:

- Desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques;
- Promover a formação e a qualificação de recursos humanos na área da cibersegurança, com vista à formação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança;
- Exercer os poderes de autoridade nacional competente em matéria de cibersegurança, relativamente ao Estado e aos operadores de infraestruturas críticas nacionais;
- Contribuir para assegurar a segurança dos sistemas de informação e comunicação do Estado e das infraestruturas críticas nacionais;
- Promover e assegurar a articulação e a cooperação entre os vários intervenientes e responsáveis nacionais na área da cibersegurança;
- Assegurar a produção de referenciais normativos em matéria de cibersegurança;
- Apoiar o desenvolvimento das capacidades técnicas, científicas e industriais, promovendo projetos de inovação e desenvolvimento na área da cibersegurança;
- Assegurar o planeamento da utilização não militar do ciberespaço em situação de crise ou de conflito armado, no âmbito do planeamento civil de emergência;
- Coordenar a cooperação internacional em matérias da cibersegurança, em articulação com o Ministério dos Negócios Estrangeiros;
- Exercer as demais competências que lhe sejam atribuídas por lei.

3.2.2 Organograma

Integram a estrutura orgânica do CNCS as seguintes equipas:

〉 **Desenvolvimento e Inovação**

A equipa multidisciplinar de Desenvolvimento e Inovação (DDI) tem como objetivo contribuir ativamente para a capacitação e promoção do capital humano, através da sensibilização e disseminação de boas práticas, da formação e treino avançado de entidades, profissionais especialistas na área e também dos jovens. O reforço da resiliência e a tomada de decisão informada, a produção de conhecimento situacional e a influência positiva sobre as políticas públicas na área da cibersegurança são também objetivos seus, assim como, a aplicação de estratégias de comunicação que fomentem o envolvimento da comunidade de interesse e o desenvolvimento de grandes eventos distribuídos geograficamente e que contribuam para o aumento da literacia, da capacitação e da promoção de redes de colaboração é outro dos propósitos do departamento.

〉 **Capacitação Técnica e Organizacional**

A equipa multidisciplinar de Capacitação Técnica e Organizacional (DCTO) tem como objetivo informar e capacitar as organizações com as melhores práticas, através de um conjunto de atividades, serviços e ferramentas desenvolvidas a pensar no crescimento e maturidade da Cibersegurança das organizações nacionais. O DCTO apoia o desenvolvimento de capacidades nas organizações através da dinamização e reforço de ações de redes de colaboração e criação de sinergias, troca de experiências e envolvimento em projetos colaborativos. Adicionalmente, tem a seu cargo a produção de documentação de apoio às organizações, sob a forma de boas práticas, guias e recomendações técnicas, prestando também apoio na sua operacionalização.

〉 **Operações:**

A equipa multidisciplinar de Operações (CERT.PT) assegura a condução da atividade operacional do CNCS que inclui as funções de coordenação nacional da resposta a incidentes no ciberespaço, de produção de relatórios de analise técnica e a produção de um quadro situacional da Cibersegurança nacional (PANORAMA) para os operadores de serviços essenciais e de infraestruturas críticas, prestadores de serviços digitais e outras organizações do Estado.

〉 **Regulação, Supervisão e Certificação**

A equipa multidisciplinar de Regulação, Supervisão e Certificação (DRSC) contempla as áreas referentes às funções de Autoridade Nacional de Cibersegurança, nos termos do n.º 4 do artigo n.º 7 da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço,

transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União Europeia, nomeadamente as de regulação e regulamentação associada, supervisão, fiscalização e sancionatórias nos termos das competências desta entidade.

O DRSC contempla ainda as áreas decorrentes do Regulamento UE 2019/881 e do Decreto-Lei n.º 65/2021, de 30 de julho, atuando também no domínio do planeamento de emergência da Cibersegurança.

〉 **Serviços Técnicos**

A equipa multidisciplinar de Serviços Técnicos (DST) presta um conjunto de serviços de suporte ao funcionamento do CNCS e do GNS, nomeadamente de gestão de infraestrutura e sistemas, de serviços informáticos de apoio ao utilizador e de operação de um SOC. Adicionalmente, este departamento produz recomendações técnicas e presta apoio às entidades nacionais na sua operacionalização.

4. Conceitos

Para efeitos do presente Manual, importa clarificar alguns conceitos tal como constam em Recomendações de organismos nacionais e Regulamentação Comunitária[1].

i. Risco

Evento, situação ou circunstância futura com a probabilidade de ocorrência e potencial consequência positiva ou negativa na consecução dos objetivos de uma unidade organizacional.

ii. Irregularidade

Qualquer violação de uma disposição de direito comunitário que resulte de um ato ou omissão de um agente económico que tenha ou possa ter por efeito lesar o orçamento geral das Comunidades ou orçamentos geridos pelas Comunidades, quer pela diminuição ou supressão de receitas provenientes de recursos próprios cobradas diretamente por conta das Comunidades, quer por uma despesa indevida.

iii. Fraude

Em matéria de despesas, define-se fraude como qualquer ato ou omissão intencionais relativos:

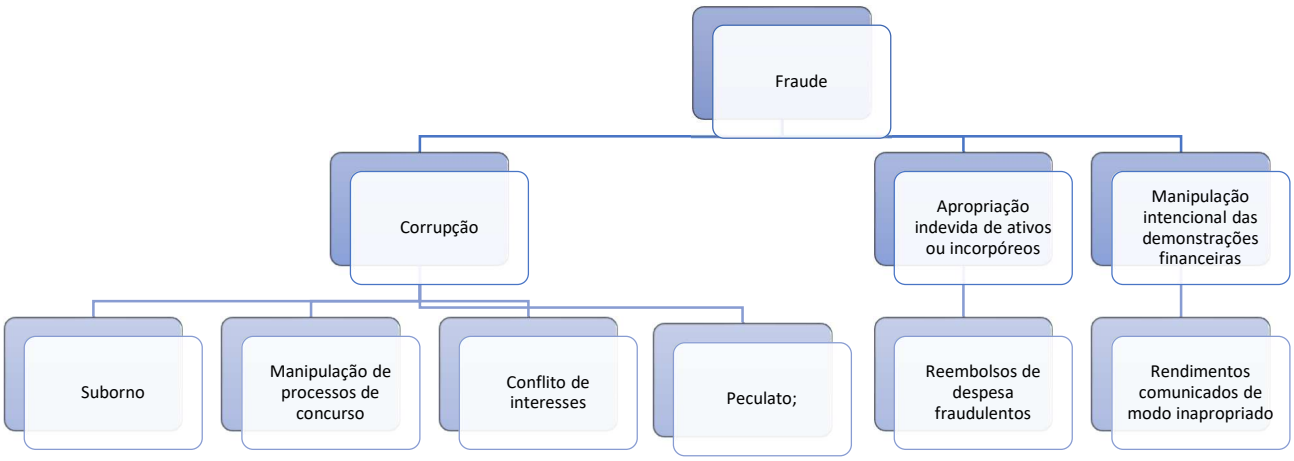
〉 À utilização ou apresentação de declarações ou de documentos falsos, inexatos ou incompletos, que tenha por efeito o recebimento ou a retenção indevida de fundos provenientes do Orçamento

[1] Destaca-se o Regulamento CE n.º 2988/95 do Conselho, de 18/12/1995, Tratado da União Europeia e Conselho de Prevenção da Corrupção.

Geral das Comunidades Europeias ou dos orçamentos geridos pelas Comunidades Europeias ou por sua conta;

- À não comunicação de uma informação em violação de uma obrigação específica, que produza o mesmo efeito;
- Ao desvio desses fundos para fins diferentes daqueles para que foram inicialmente concedidos.

Será de relevar que o carácter intencional é o que distingue o conceito de fraude de irregularidade. Na *Information Note on Fraud Indicators for ERDF, ESF and CF (COCOF 09/0003/00-EN, de 18/02/2009)*, a Comissão Europeia utiliza a classificação de tipos de fraude da Association of Certified Fraud Examiners, que considera a existência de três tipos de fraude:



iv. Corrupção

A corrupção consiste na prática de um qualquer ato ou a sua omissão, seja lícito ou ilícito, contra o recebimento ou a promessa de uma qualquer compensação que não seja devida, para o próprio ou para terceiro.

A corrupção na aceção do artigo 136.º do º do Regulamento (EU, Euratom) 2018/1046, de 18 de julho distingue-se entre:

- **Passiva -** o facto de um funcionário, intencionalmente, de forma direta ou por interposta pessoa, solicitar ou receber vantagens de qualquer natureza, para si próprio ou para terceiros, ou aceitar a promessa dessas vantagens, para que pratique ou se abstenha de praticar, em violação dos deveres do seu cargo, atos que caibam nas suas funções ou no exercício das mesmas e que lesem ou sejam suscetíveis de lesar os interesses financeiros das Comunidades Europeias;
- **Ativa -** o facto de uma pessoa prometer ou dar intencionalmente, de forma direta ou por interposta pessoa, uma vantagem de qualquer natureza a um funcionário, para este ou para terceiros, para que pratique ou se abstenha de praticar, em violação dos deveres do seu cargo,

atos que caibam nas suas funções ou no exercício das mesmas e que lesem ou sejam suscetíveis de lesar os interesses financeiros das Comunidades Europeias.

v. Crimes Conexos

Trafico de influências	Consiste na prática ilegal de uma pessoa se aproveitar da sua posição privilegiada dentro de uma empresa ou entidade, ou das suas conexões com pessoas em posição de autoridade, para obter favores ou benefícios para terceiros, geralmente em troca de favores ou pagamento.
Peculato	Em razão do cargo, o trabalhador tem a posse de coisa móvel pertencente à administração pública ou sob a guarda desta (a qualquer título), e dela se apropria, ou a distrai do seu destino, em proveito próprio ou de outrem.
Concussão	É o ato de exigir para si ou para outrem, dinheiro ou vantagem em razão da função, direta ou indiretamente, ainda que fora da função ou antes de assumi-la, mas em razão dela, vantagem indevida.
Suborno	É a prática de prometer, oferecer ou pagar a uma autoridade, governante, funcionário público ou profissional da iniciativa privada qualquer quantidade de dinheiro ou quaisquer outros favores para que a pessoa em questão deixe de se portar eticamente com seus deveres profissionais.
Participação económica em negócio	Preenche o crime de participação económica em negócio o trabalhador que, no exercício das suas funções públicas, ao invés de atuar como zelador do interesse público que lhe está confiado, abusa dos poderes conferidos pela titularidade do cargo com finalidade lucrativa para si ou para terceiro.
Abuso de poder	É o ato ou efeito de impor a vontade de um sobre a de outro, tendo por base o exercício do poder, sem considerar as leis vigentes.

vi. Conflito de Interesses

De acordo com o artigo 61.º do Regulamento Financeiro[2] existe conflito de interesses quando o "*exercício imparcial e objetivo das funções de um ator financeiro ou outra pessoa" envolvido na execução financeira "estiver comprometido por razões que envolvam família, vida emocional, afinidade política ou nacional, interesse económico ou qualquer outro interesse pessoal direto ou indireto*".

No desempenho de funções, os colaboradores do GNS e do CNCS devem garantir que não participam em processos de decisão nos quais estejam diretas ou indiretamente, envolvidas entidades com quem tenham colaborado ou que estejam (ou tenham estado) ligados por laços de parentesco ou outros.

No que concerne à potencial existência de conflito de interesses, entende-se que ela existe quando os colaboradores do GNS/CNCS se encontrem numa situação em virtude da qual se possa, com razoabilidade, duvidar seriamente da imparcialidade da sua conduta ou decisão, nos termos dos artigos 69º a 73º do Código do Procedimentos Administrativo.

Assim, os funcionários civis e militares, e colaboradores do GNS/CNCS, no desempenho de funções, devem garantir que não participam em atos preparatórios nem processos de decisão ou de auditoria ou de controlo nos quais estejam, direta ou indiretamente, envolvidas entidades com quem tenham colaborado ou que estejam (ou tenham estado) ligados por laços de parentesco ou outros.

A situação de conflito de interesses abrange os períodos que antecedem e sucedem o exercício de funções públicas, pelo que os titulares de órgãos da Administração pública e os respetivos agentes, bem como quaisquer outras entidades que, independentemente da sua natureza, se encontrem no exercício de poderes públicos, não podem intervir em procedimento administrativo ou em ato ou contrato de direito público ou privado da Administração Pública, que hajam prestado serviços, há menos de três anos, a qualquer dos sujeitos privados participantes na relação jurídica procedimental (vide números 1 e 3 do artigo 69º. do Código do Procedimentos Administrativo).

Os colaboradores do GNS/CNCS não podem exercer qualquer atividade externa que interfira com as funções que desempenham no GNS/CNCS evitando, desse modo, incorrer em qualquer situação de conflito de interesses, seus ou de terceiros, que por essa via prejudiquem ou venham a prejudicar a decisão

[2] Regulamento (EU, Euratom) 2018/1046, do Parlamento Europeu e do Conselho, de 18 julho de 2018 e Comunicação da Comissão Europeia, contendo Orientações sobre a Prevenção e gestão de conflito de interesses no quadro do Regulamento Financeiro (2021/C 121/01).

e o rigor nas decisões administrativas e levar à presunção de existência de falta de imparcialidade da sua atuação, no exercício das suas atividades.

Os colaboradores do GNS/CNCS podem acumular funções ou atividades exclusivamente nos termos legalmente estabelecidos e devidamente autorizadas, dependendo de comunicação escrita ao superior hierárquico, para análise e verificação de incompatibilidades, caso a caso.

Os colaboradores do GNS/CNCS que se encontram em regime de acumulações de funções devem, assim, declarar por escrito, aos respetivos superiores hierárquicos, que as atividades que desenvolvem não colidem, sob forma alguma, com as funções públicas que desempenham no GNS/CNCS, nem colocam em causa a isenção e o rigor que pautam a sua atuação. A resolução de conflitos de interesses deve respeitar escrupulosamente as disposições legais, regulamentares e contratuais aplicáveis.

Os funcionários civis e militares, e colaboradores da GNS/CNCS não podem intervir na apreciação nem no processo de decisão, sempre que estiverem em causa procedimentos administrativos de qualquer natureza, que possam afetar, ou em que possam estar em causa, interesses particulares seus ou de terceiros, e que por essa via prejudiquem ou possam prejudicar a isenção e o rigor das decisões administrativas que tenham de ser tomadas, ou que possam suscitar a mera dúvida sobre a isenção e o rigor que são devidos ao exercício de funções públicas.

Como tal, quer os colaboradores, quer os prestadores de serviço que contratualmente colaborem com o GNS/CNCS, devem subscrever a declaração individualizada de inexistência de conflitos de Interesses, conforme o modelo constante no Código de Conduta do GNS (Anexo I - Declaração de Inexistência de Conflito de Interesses), em cada processo/ação/investimento/contrato em que intervenham, a qual deve ser junta à ficha técnica do processo/ação/investimento/contrato, na qual se identificam todos os elementos intervenientes.

Os colaboradores do GNS/CNCS que, no exercício das suas funções, estejam perante uma situação passível de configurar um conflito de interesses, devem subscrever declaração individualizada de conflito de interesses, declarando-se impedidos e solicitando escusa do desempenho das funções atribuídas na sua atividade, comprometendo-se a comunicar tal facto, de imediato, ao seu superior hierárquico, conforme o modelo constante no Código de Conduta do GNS.

5. Instrumentos de Mitigação dos Riscos de Fraude

Para uma adequada gestão e prevenção de potenciais riscos de fraude, o GNS/CNCS, elaborou e adotou diversos instrumentos de mitigação de riscos, decorrentes de exigências legais nacionais e comunitárias.

Enquanto beneficiário do PRR, o GNS/CNCS é obrigado a garantir que os seus procedimentos internos se encontram objetivados em:

- Descrição do Sistema de Gestão e Controlo Interno;
- Manuais de Procedimentos;
- Orientações Técnicas.

O Regime Geral de Prevenção da Corrupção (doravante designado "*RGPC*"), em anexo ao Decreto-Lei n.º 109/E-2021, de 9 de dezembro, também estabelece a obrigatoriedade do GNS/CNCS adotar, como medidas preventivas de risco de fraude, um conjunto de instrumentos essenciais que contribuem para uma política de prevenção e sensibilização dos potenciais riscos de fraude, nomeadamente:

- Código de Ética e Conduta;
- Declaração de Política Antifraude;
- Plano de Gestão de Riscos e Infrações Conexas;
- Declaração de Inexistência de Conflito de Interesses.

Neste sentido o GNS e o CNCS divulgam nas suas páginas da internet os documentos elencados cumprindo com este desígnio legal.

Este enquadramento permite considerar que o GNS/CNCS dispõe de meios adequados a uma gestão preventiva e atempada de potenciais riscos de fraude garantindo ao PRR um nível tolerável de exposição ao risco.

5.1 Tratamento de denúncias

No âmbito do Programa de Cumprimento Normativo, foi criado o Canal de Denúncias interno do GNS/CNCS como mecanismo de prevenção, deteção e sancionamento de atos de corrupção e infrações conexas, levados a cabo contra ou através da entidade (*vide* n.º 1 do artigo 5.º e artigo 8.º do RGPC, aprovado em anexo ao Decreto-Lei n.º 109-E/2021, de 9 de dezembro), o qual se encontra disponível na página da internet do GNS e do CNCS.

Para garantir a conformidade da implementação do canal de denúncias, a Lei n.º 93/2021, de 20 de dezembro estabelece o Regime Geral de Proteção de Denunciantes de Infrações (doravante designada "*RGPDI*") e procede à transposição da Diretiva (UE) 2019/1937, do Parlamento Europeu e do Conselho, de 23 de outubro, relativa à proteção das pessoas que denunciam violações do direito da União) e concretiza os requisitos e procedimentos a adotar nos canais de denúncias.

O canal de denúncia do GNS é um meio de comunicação seguro de denúncias que assume um carácter, essencialmente, preventivo, uma vez que é um instrumento de autorregulação e autocontrolo

que permitirá ao GNS, perante factos conhecidos e relatados de boa-fé, atuar e corrigir eventuais atuações ilícitas e prevenir a sua ocorrência futura, garantindo o cumprimento da lei, regulamentos e procedimentos em vigor, tratando-se de uma atuação exclusivamente orientada para a prossecução do interesse público.

Na mesma linha, foi aprovado o manual de procedimentos do Canal de Denúncias onde se encontram definidos, nomeadamente, os termos da sua receção, registo e encaminhamento, respetiva análise, comunicação da decisão final e, ainda, o direito de informação, consulta do processo e passagem de certidões.

As denúncias recebidas no GNS são tratadas de acordo com o previsto na Lei n.º 58/2019, de 08 de agosto, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e de acordo com o Regime de Proteção de Denunciantes de Infrações, estabelecido pela Lei n.º 93/2021, de 20 de dezembro, e demais legislação sobre a matéria.

O canal é operado internamente, cabendo exclusivamente aos trabalhadores indicados para o efeito (núcleo de assessoria jurídica) a receção e seguimento de denúncias efetuadas, a quem compete desenvolver as atividades adequadas à verificação das alegações contidas na denúncia e, se for caso disso, promover a cessação da infração denunciada, inclusive através da abertura de um inquérito interno ou da comunicação a autoridade competente para investigação da infração, incluindo as instituições, órgãos ou organismos da União Europeia.

6. Metodologia de Avaliação dos Riscos de Fraude

Como forma de avaliar a incidência e a probabilidade de ocorrência de riscos de fraude, o GNS/CNCS recorre à ferramenta de avaliação de risco de fraude disponibilizada pela Comissão Europeia, a qual assenta nas seguintes etapas metodológicas:

1. Quantificação da probabilidade e do impacto de um determinado risco de fraude - Risco Bruto;
2. Avaliação da eficácia dos controlos atualmente implementados na mitigação do Risco Bruto;
3. Avaliação do Risco Residual após o efeito dos controlos atuais e da sua eficácia, ou seja, a situação tal como é atualmente;
4. Avaliação do efeito dos controlos planeados no Risco Residual;
5. Definição do Risco Alvo, ou seja, do nível que o GNS/CNCS considera tolerável.

Assim, partindo dos riscos identificados em cada uma das atividades suscetíveis de comportarem riscos de fraude, através da ferramenta em causa, o GNS/CNCS, procede à identificação dos mecanismos de controlo associados a cada uma das atividades de risco.

A ferramenta de autoavaliação de risco que irá suportar a aplicação desta metodologia pelo ao GNS/CNCS integra como Anexo deste Manual.

Todo o processo de avaliação é devidamente documentado, o que permitirá, sempre que necessário, uma revisão das conclusões obtidas.

6.1 Atividades com Maior Vulnerabilidade à Incidência de Risco de Fraude

Na "*Guidance for Member States and Programme Authorities on fraud risk assessment and effective and proportionate anti-fraud measures*" a Comissão Europeia identifica quatro processos-chave e transpôs para uma ferramenta de avaliação de risco de fraude um conjunto de situações de risco pré-definidas que devem ser alvo de avaliação pelas autoridades de gestão:

- Seleção de candidaturas;
- Execução e verificação de operações;
- Validação de despesas e pagamentos;
- Procedimentos de contratação pública.

Dando sequência a estas orientações, o GNS/CNCS, com as necessárias adaptações, , mas sim de contratualização com beneficiários diretos e intermediários identificou riscos em torno de dois processos chave que se consideram de maior vulnerabilidade à incidência de risco de fraude, designadamente:

- Contratualização:
    1. Conflito de Interesses dos Colaboradores com responsabilidade pela contratualização;
    2. Falsas declarações prestadas pelos beneficiários indiretos;
    3. Duplo Financiamento.
- Execução e Verificação das Operações:
    1. Riscos dos contratos públicos adjudicados;
    2. Conflitos de interesses não declarados, subornos e comissões ilegais;
    3. Adoção de procedimentos que violem o princípio da concorrência;
    4. Preços (orçamentos) inadequados;
    5. Manipulação dos orçamentos e da faturação;
    6. Alterações contratuais;

Além deste conjunto de situações de risco pré-definidas, o GNS/CNCS, em sede de autoavaliação e monitorização da avaliação de risco, poderá vir a integrar novas situações de risco que venham a ser identificadas e que se justifiquem ser objeto de uma avaliação de risco de fraude.

6.2 Avaliação e Monitorização

O presente Manual, bem como a execução das medidas preventivas de risco propostas, é objeto de uma avaliação, a realizar no final de cada ano civil durante o período de execução do PRR sempre que ocorram alterações significativas ao sistema de gestão e controlo, elaborando-se subsequentemente um relatório com as conclusões obtidas.

Das conclusões obtidas destaca-se a obrigatoriedade de constar a apreciação sobre a necessidade, ou não, da revisão do Manual de Gestão do Risco. Ocorrendo a revisão, o Manual atualizado é então remetido para aprovação e posteriormente divulgado.

Sempre que, da avaliação efetuada, resulte a implementação de um plano de ação para a concretização de medidas antifraude eficazes e proporcionadas, procede-se à identificação do responsável pela execução efetiva desse plano e à definição do prazo da sua implementação.

7. Divulgação do Manual e Relatório de Avaliação

O presente Manual, bem como os resultados da aplicação da metodologia, ou seja, o relatório de autoavaliação anual, são divulgados internamente junto dos colaboradores do GNS/CNCS e externamente enviado à EMRP, para o endereço de email avaliacaoriscofraude@recuperarportugal.gov.pt, bem como nas páginas eletrónicas institucionais.

ANEXO I – FICHA DE AUTOAVALIAÇÃO DE RISCO DE FRAUDE

O nível de risco é uma combinação do grau de probabilidade com a gravidade da consequência da respetiva ocorrência. Seguindo a metodologia adotada pela Inspeção-Geral de Finanças (IGF) – Autoridade da Auditoria, no seu próprio plano, o grau de risco pode ser classificado de acordo com três categorias: "Elevado", "Moderado" ou "Fraco", em função de duas variáveis que integram as definições de risco:

- Probabilidade de ocorrência das situações que comportam "risco";
- Impacto estimado das infrações.

Da conjugação destas variáveis apresenta-se a seguinte tabela, com os graus de risco que serão adotados no presente Plano.

1) Qualificação do risco

Tabela de Risco	Probabilidade de Ocorrência			
		Elevado 3	**Moderado 2**	**Fraco 1**
Impacto da Ocorrência	**Elevado 3**	Elevado 9	Moderado 6	Fraco 3
	Moderado 2	Moderado 6	Moderado 4	Fraco 2
	Fraco 1	Fraco 3	Fraco 2	Fraco 1

Legenda:

Elevado	>= 7
Moderado	>=4 e <=6
Fraco	<=4

2) Critérios de Graduação

Impacto da ocorrência

Elevado (3)	**Moderado** (2)	**Fraco** (1)
Prejuízos financeiros significativos para o Estado Português ou para os interesses financeiros da União e a violação grave dos princípios associados ao interesse público, lesando a credibilidade do GNS/CNCS.	Prejuízos reputacionais, operacionais, financeiros e/ou regulatórios para o Estado Português ou para os interesses financeiros da União e perturbação do normal funcionamento do GNS/CNCS.	Não tem potencial para provocar prejuízos reputacionais, operacionais, financeiros e/ou regulatórios ao Estado Português ou aos interesses financeiros da União, não sendo as infrações causadoras de danos relevantes na imagem e operacionalidade do GNS/ CNCS.

Probabilidade da ocorrência

Elevado (3)	**Moderado** (2)	**Fraco** (1)
O risco decorre de um processo corrente e frequente do GNS e/ou do CNCS.	O risco está associado a um processo esporádico do GNS e/ou do CNCS que se admite venha a ocorrer ao longo do ano.	O risco decorre de um processo que apenas ocorrerá em circunstâncias excecionais.

Identificação dos Riscos, Graduação e Medidas de Prevenção

Tendo em conta as atribuições do GNS/CNCS e as competências das diferentes, equipas multidisciplinares foram identificadas e caracterizadas, os potenciais riscos de corrupção e infrações conexas. Conforme referido no antecedente ponto "Qualificação do Risco", estes riscos foram classificados segundo uma escala de risco elevado, moderado e fraco, em função do grau de probabilidade de ocorrência e do seu impacto. Identificados os riscos, foram indicados os mecanismos de controlo interno existentes para prevenir a sua ocorrência, propondo-se, em alguns casos, medidas adicionais consideradas adequadas.

(Ficha de Autoavaliação de Risco de Fraude consta do ficheiro Excel em Apêndice)