GABINETE NACIONAL DE SEGURANÇA
E
CENTRO NACIONAL DE CIBERSEGURANÇA

Plano de Atividades

2024

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

PÁGINA DEIXADA EM BRANCO

ÍNDICE

SUMÁRIO EXECUTIVO

O planeamento das atividades a desenvolver em 2024 é enquadrado pelo diploma orgânico do Gabinete Nacional de Segurança (GNS) – Decreto-Lei nº 3/2012, de 16 de janeiro, **republicado** pelo Decreto-Lei nº 136/2017, de 06 de novembro **e alterado pelo Decreto-Lei n.º 139-A/2023, de 29 de dezembro**, e tendo em conta as orientações estratégicas superiormente definidas para o triénio 2023/2026. Destaca-se ainda a necessidade da execução das medidas e marcos/metas do investimento TD C19 i03 do PRR planeadas para este ano e iniciativas afins, em harmonia com os objetivos vertidos no programa do XXIII Governo Constitucional, no que se relaciona com a Missão do GNS e do CNCS e com a flexibilidade suficiente para uma rápida adaptação à volatilidade da envolvente geoestratégica.

O GNS/CNCS dará continuidade à concretização do seu plano estratégico para o triénio 2023/2026, consubstanciando a respetiva visão "Contribuir para um Portugal mais seguro, através de um comportamento confiável, preventivo, em rede e inovador" e centrada no serviço aos Públicos de Interesse, através da concretização de uma política e prática de cultura de segurança da informação em estreita articulação institucional, o que tem permitido contornar e mitigar as contingências inerentes à origem, estatuto e enquadramento laboral do pessoal em serviço. Para este resultado positivo contribuirá, de forma decisiva, o facto de, na sua quase totalidade, os recursos humanos do GNS provirem das Forças Armadas e das Forças de Segurança, entidades que vêm continuando a assegurar o pagamento dos encargos remuneratórios e subsídios de alimentação.

Relativamente ao CNCS, ter-se-á, dentro do possível, de prosseguir com o incremento da equipa afeta ao Centro, num quadro de grande procura por pessoas com competências na área da cibersegurança, quer no setor público quer, sobretudo, no setor privado.

Dos objetivos estratégicos decorrem um conjunto de objetivos operacionais (servidos por indicadores e metas), com carácter transformacional, que visam garantir a orientação para os resultados, bem como um conjunto de indicadores e respetivas métricas que refletem as atividades correntes e essenciais ao funcionamento do GNS/CNCS. Pretende-se que todas as unidades orgânicas e áreas funcionais do GNS/CNCS estejam enquadradas na estratégia definida.

A visão e os valores, princípios que orientam a atividade do GNS/CNCS, encontram-se ajustados a uma organização que se pretende resiliente, mas com capacidade de aprender e inovar, e entregando, de forma previsível e eficaz, os serviços e produtos que tem de proporcionar aos públicos de interesse.

Em 2024, pretende-se levar a efeito um conjunto de ações que visam reforçar a consolidação dos projetos e processos anteriormente iniciados, nomeadamente a prossecução da desmaterialização dos processos internos e a consolidação da estrutura e dos processos inspetivos executados pelo GNS, visando uma maior proximidade às entidades sujeitas a inspeção. Todas estas iniciativas deverão ser desenvolvidas com o digital por defeito, centrado nos públicos de interesse (pessoas que fazem parte do GNS e CNCS) e com forte pendor de inovação.

Para o efeito, é indispensável um adequado nível e maturidade de colaboradores, pelo que é necessário reforçar os recursos humanos, sendo objetivo do GNS/CNCS atingir, no final de 2024, um quantitativo global de 156 trabalhadores, dos quais 71 no Centro Nacional de Cibersegurança (CNCS).

Em termos financeiros, a dotação inicial do orçamento de funcionamento do GNS/CNCS é de € 6.611.900 dos quais € 4.249.951 são respeitantes à atividade do CNCS. No âmbito do Plano de Recuperação e Resiliência está previsto um investimento de € 16.181.019. A Lei do OE-2024 e o subsequente decreto-lei de execução orçamental contemplam cativações (até à data foram aplicadas cativações no valor de € 561.429) e reduções adicionais, pelo que poderá assim vir a tornar-se necessário adequar o presente Plano de Atividades à realidade financeira que vier a impor-se no decurso da execução do OE de 2024.

Em conclusão, para o ano de 2024, o foco será a execução das medidas e marcos/metas do investimento "Reforço do Quadro Geral de Segurança e Ciberbersegurança, na base da confiança para a adoção dos serviços electrónicos" – TD C19-i03 no âmbito do PRR, retendo a flexibilidade suficiente para uma rápida adaptação à volatilidade da envolvente geoestratégica.

No que ao atual plano estratégico diz respeito deverá prosseguir-se com um esforço especial em três áreas, designadamente:

- **Genética –** onde se pretende aumentar os recursos humanos e adequar as infraestruturas para os acomodar, recorrendo às medidas previstas no PRR;
- **Estrutural –** em que se pretende otimizar os processos associados à contratação de pessoas, bens de serviço através da melhoria e modernização dos processos e tecnologias afetos ao controlo de gestão interno;
- **Públicos de Interesse –** através da maximização da execução do PRR, operacionalização da NIS2 e modernizar a moldura legislativa para a tramitação da informação classificada.

A concretização destes desideratos permitirá dar espaço à inovação para modernizar as capacidades do GNS e do CNCS, contribuindo assim para o incremento da segurança em Portugal.

NOTA INTRODUTÓRIA

O Gabinete Nacional de Segurança é um "serviço central da administração direta do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar".

A sua **MISSÃO**, nos termos do n.º 1 do artigo 2.º do Decreto-Lei n.º 3/2012 de 16 de Janeiro, **republicado** pelo Decreto-Lei nº 136/2017, de 06 de novembro **e alterado pelo Decreto-Lei n.º 139-A/2023, de 29 de dezembro**, é "(…) garantir a segurança da informação classificada 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 informação classificada, 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.".

O CNCS, nos termos do n.º 2 do mesmo Artigo e Decreto-Lei supra referido, funciona no âmbito do GNS, tendo como missão "(…) contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais".

Os **VALORES** de uma organização são os padrões de conduta que norteiam o comportamento dos trabalhadores e da organização. O GNS/CNCS identifica como seus valores específicos os seguintes:

- **Lealdade:** professada na prática da verdade, da fidelidade aos princípios éticos, e da constância e firmeza no compromisso assumido para com as chefias, para consigo mesmo e para com os seus pares. Pressupõe a confiança nas decisões dos superiores, no apoio dos pares ao esforço coletivo e no trabalho dos colaboradores.
- **Confiabilidade**: capacidade de dar resposta às solicitações externas nos prazos determinados, mesmo em circunstâncias adversas e inesperadas.
- **Honestidade**: ato de ser honesto, de ser verdadeiro. É virtude que exige coerência e sinceridade no agir, sentir e falar.
- **Rigor**: fazer com seriedade de princípios, exatidão, precisão, concisão e pontualidade.
- **Honra:** percecionada na conduta virtuosa, na firmeza e na dignidade de carácter. Espelha honestidade, respeito e seriedade, e reflete-se no reconhecimento público que se obtém pelo cumprimento do dever, donde resulta reputação e prestígio.
- **Integridade**: assunção de responsabilidades, materializada na transparência, honestidade e justeza das decisões e atos. Tem como retorno o respeito e a confiança dos outros.

A **VISÃO** é a descrição do futuro desejado para a organização. Esse enunciado reflete o alvo a ser procurado mediante os esforços individuais, esforços das equipas e pela alocação dos recursos.

O GNS e o CNCS pretendem ser conhecidos como organizações confiáveis, mantendo uma boa reputação percecionada pelos públicos de interesse no âmbito do cumprimento da missão institucional, com a capacidade para se adaptarem com rapidez às condições da mudança constante, pensando como organizações aprendentes, antecipando soluções para os novos desafios que se colocam no cumprimento da missão, com vista à adaptação às novas realidades, colaborando com entidades que constituem os seus públicos de interesse e que inovam, e procurando fazer diferente, através da criação de novos

produtos/serviços e métodos de trabalho, antecipando as necessidades/expectativas da comunidade servida.

Assim, a **VISÃO** do GNS/CNCS pode ser traduzida em "Contribuir para um Portugal mais seguro, através de um comportamento confiável, preventivo, em rede e inovador."

Em 2024, o GNS/CNCS pretende dar continuidade e concluir um conjunto de ações, de grande visibilidade externa, prosseguindo com a continuidade da regulamentação setorial do regime jurídico de Segurança do Ciberespaço (Lei nº 46/2018, de 13 de agosto) e a implementação dos respetivos mecanismos de supervisão, bem como da implementação da componente nacional do mecanismo europeu de certificação em Cibersegurança, previsto no Regulamento (UE) 2019/881; no âmbito da ação externa, a promoção de sessões de discussão pública do Projeto de Lei de Segurança da Informação Classificada (LSIC); fazer evoluir o modelo de formação sobre a gestão do ciclo da vida da Informação Classificada (IC), reforçando e diversificando os conteúdos do atual modelo misto (e-learning + presencial), e cuja frequência passará a constituir um requisito para a credenciação, renovação e elevação de pessoas singulares; no âmbito da formação, a prossecução com a modernização da forma como estas entidades estão presentes no ciberespaço, através dos canais de comunicação digital, prosseguindo com a execução do Programa de Formação Avançada em Cibersegurança (C-ACADEMY), a realização de atividades de sensibilização do cidadão no âmbito do Centro Internet Segura e de capacitação das organizações em Cibersegurança, nomeadamente, através de uma rede centros de competências (C-NETWORK), do Polo de inovação digital em Cibersegurança; no âmbito da simplificação da interação com os públicos de interesse, concluir a projeção dos novos Sistemas de Segurança Eletrónica da Informação (SEIF) e de Gestão do Ciclo de Vida de Material Cripto (SCRIPTO) e continuar a capacitar a Equipa Nacional CERT.PT com os instrumentos e as ferramentas necessárias para incrementar a sua capacidade de operar e comunicar com a comunidade e autoridades públicas de cibersegurança.

ESTRATÉGIA E OBJETIVOS

O Plano de Atividades, que se encontra alinhado com o plano estratégico para o triénio 2023/2026, constitui-se como um referencial de gestão e administração do GNS e do CNCS para o ano de 2024, tendo em conta as respetivas natureza, missão e atribuições.

Os objetivos estratégicos definidos decompõem-se em linhas de ação que visam prosseguir com a edificação equilibrada de capacidades, incluindo a respetiva sustentação, prosseguir com a otimização processual e organizacional, e empregar as capacidades para melhor cumprir a missão do GNS/CNCS.

Cada objetivo estratégico possui um conjunto de ações (objetivos operacionais), a que correspondem um conjunto de iniciativas/projetos, que contribuirão para que se atinja o respetivo objetivo estratégico com sucesso.

Na elaboração do plano de atividades procurou-se assegurar a efetiva participação de elementos do GNS e do CNCS, iniciada com uma aproximação top/down, com a transmissão da estratégia, seguido do procedimento bottom/up, com a definição dos objetivos operacionais. Com este procedimento procurou-se que todas as unidades orgânicas estivessem envolvidas com a formulação deste importante documento de gestão e assim alinhadas com a estratégia definida para o GNS/CNCS.

Para 2024, foram selecionados, para constarem no QUAR, os seguintes objetivos estratégicos:

OE1: Robustecer a capacidade de conhecimento do Ciberespaço para a proteção da sociedade.

OE2: Desenvolver competências na área da Informação Classificada que contribuam para uma melhor resposta às necessidades emergentes.

OE3: Consolidar a qualidade da prestação de serviços.

OE4: Investir na formação e no bem-estar das pessoas trabalhadoras.

Destes objetivos estratégicos decorrem 2 do GNS, 2 do CNCS bem como os respetivos objetivos operacionais, inscritos no QUAR-2024, cuja concretização será obtida mediante a realização das atividades de cada uma das unidades orgânicas.

Os OE encontram-se alinhados com o Programa do XXIII Governo Constitucional, designadamente com o desafio estratégico (DE) da construção de uma sociedade digital, da criatividade e da inovação (4º DE) enquadrado pelos princípios enunciados para a boa governação, designadamente Contas Certas para a recuperação e convergência, Investir na Qualidade dos Serviços Públicos, Melhorar a Qualidade da Democracia e Valorizar Funções de Soberania.

ATIVIDADES E RECURSOS

Para se atingirem os objetivos definidos, torna-se necessário desenvolver um conjunto de ações cuja concretização permite atingir os objetivos fixados, estratégicos e operacionais.

A concretização dos objetivos em todas as perspetivas, devidamente articulados entre si, em termos de causa efeito, constitui a base para se atingirem os objetivos estratégicos fixados.

Assim, a concretização dos objetivos operacionais será obtida mediante a realização das atividades identificadas para cada uma das unidades orgânicas do GNS e do CNCS.

Decorrendo da missão do GNS, as principais atividades desenvolvidas são a credenciação de:

(i) segurança de pessoas singulares ou coletivas para administração de informação classificada;
(ii) entidades de certificação eletrónica do Estado;
(iii) segurança a entidades para o exercício de atividades industriais, tecnológicas e de investigação;
(iv) segurança nacional às empresas de comércio e indústria de bens e tecnologias militares;
(v) certificação de segurança a produtos e sistemas de comunicações, de informática e de tecnologias de informação classificada, certificação das entidades gestoras de plataformas eletrónicas de contratação pública e supervisão da implementação do regulamento 910/2014 da UE.

Quanto ao CNCS, as principais atividades centram-se no desenvolvimento das capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques, no processo de operacionalização da Lei 46/2018 de 13 de agosto que transpõe a Diretiva de Segurança das Redes da Informação (Diretiva SRI) para a legislação nacional, e na coordenação do plano de ação da Estratégia Nacional de Cibersegurança (ENSC).

Com a publicação do DL 65/2021 de 30 de julho, que Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança, o CNCS reforçou as suas competências enquanto Autoridade Nacional de Certificação de Cibersegurança.

GABINETE NACIONAL DE SEGURANÇA

DEPARTAMENTO DE INSPEÇÃO E AUDITORIA (IA)

O Departamento de Inspeção e Auditoria 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 e do CNCS, assim como o cumprimento de legislação aplicável ao GNS e ao CNCS.

OBJETIVOS OPERACIONAIS

IA_G201- Desenvolver um Sistema de Gestão e Controlo da Atividade Inspetiva e de Auditoria (GAIA) **(Objetivo operacional do QUAR 2024 – RELEVANTE)**

Indicador: Percentagem de implementação do Projeto GAIA (De acordo com "Plano de Desenvolvimento e Implementação".

Meta: 80%

IA_G202 - Assegurar a implementação do Regime Geral de Prevenção da Corrupção (RGPC).

Indicador 1: Número de pontos de situação do Plano de Prevenção de Risco de Corrupção e Infrações Conexas (PPRCIC).

Meta: 2 (março, setembro).

Indicador 2: Número de Relatórios referentes ao Plano de Prevenção de Risco de Corrupção e Infrações Conexas (PPRCIC).

Meta: 2 (Relatório de avaliação anual (abril) e Relatório de avaliação intercalar (outubro)).

Indicador 3: Resposta tempestiva às denúncias apresentadas (dentro do prazo previsto no manual de procedimentos do Canal de Denúncias).

Meta: 100%

Indicador 4: Concretização do Plano de Formação e Comunicação.

Meta 1: 2 sessões de divulgação.

Meta 2: Frequência de ações de formação (um elemento de cada unidade orgânica).

Meta 3: Inclusão de referências a todos os instrumentos do Regime Geral de Prevenção da Corrupção no Manual de Acolhimento.

IA101- Realizar e coordenar a atividade inspetiva no território nacional.

Indicador: Número de Inspeções.

Meta: 25.

IA102- Realizar e coordenar a atividade inspetiva internacional.

Indicador: Número de Inspeções a Embaixadas e Postos Diplomáticos.

Meta: 3.

DEPARTAMENTO DE DOUTRINA E FORMAÇÃO (DF)

O Departamento de Doutrina e Formação desenvolve um conjunto de atividades centradas na dinamização de competências que visam a salvaguarda da Informação Classificada (IC). Neste contexto, o DDF estabeleceu como objetivos operacionais para 2024, o desenvolvimento e implementação de formação, no formato e-learning, para o refrescamento e reforço dos temas abordados no Curso de Introdução à Segurança da Informação Classificada (CISIC), destinada à frequência pelos sujeitos que já tendo a formação de base, por via das suas funções, necessitem de ver renovada a sua credenciação de segurança.

Em simultâneo, estabelecem-se os objetivos de alojamento na plataforma NAU e respetiva operacionalização do curso em formato e-learning, no âmbito do sistema seguro de troca de informação entre os órgãos de segurança e a consolidação na formação com casos práticos de forma a contribuir, para o cumprimento das políticas de segurança, procurando paralelamente, manter os elevados índices de satisfação.

O Departamento de DF elege e destaca nas suas atividades para 2024, o incremento da cultura de segurança e o desenvolvimento e atualização das respetivas políticas, com a materialização de ações de formação e sensibilização realizadas para todas as entidades que necessitem consolidar os conceitos ligados à proteção de Informação Classificada e, através do seu núcleo de Doutrina, a representação do GNS nos fóruns onde as políticas de segurança são discutidas, nomeadamente nos Comités (Security Committee) da NATO e da EU, promovendo a atualidade de todo o normativo nacional (Normas Técnicas). Desenvolve também, as atividades não discriminadas relativas à celebração e atualização de acordos bilaterais com outros estados

para a proteção mútua de IC. A DF persegue ainda a atividade de discussão pública da atualização do Quadro Legal do GNS, tema inadiável e que almeja a substituição dos SEGNAC (Segurança Nacional) vigentes, na forma de Resoluções de Concelhos de Ministros.

OBJETIVOS OPERACIONAIS

DF_P101 – Disponibilizar um curso sobre Segurança da Informação Classificada, num modelo de e-learning, através da execução de contrato para o seu desenvolvimento.

Indicador: Execução do contrato.

Meta: 31 de dezembro

DF_P101.1 – Assegurar a disponibilização do curso destinado ao refrescamento do Curso de Introdução à Segurança da Informação Classificada, tendo em vista a habilitação para o início do processo de revalidação de credenciações de segurança.

Indicador: Disponilização do Curso.

Meta: Final do primeiro semestre

DF_PI101 – Assegurar a formação no âmbito da Segurança da Informação Classificada, através da realização de duas ações de formação, a realizar no primeiro e segundo semestre.

Indicador: Satisfação global média (%) do curso, atribuída pelos participantes.

Meta: >= 85%.

INDICADORES DE ATIVIDADE

IA103 – Ações de formação. Promover ações de sensibilização para uma cultura de Segurança.

Indicador: Número de ações realizadas.

Meta: 8.

IA104 – Promover a discussão publica do projeto de LSIC.

Indicador: Promover sessões de discussão pública do Projeto de Lei de Segurança da Informação Classificada (LSIC).

Indicador: Número de sessões realizadas.

IA105 – Doutrina (NATO; União Europeia; Nacional).

Indicador: Participação em reuniões no âmbito da NATO Security Committee e do Council Security Committee. 8 reuniões

IA106 –Acordos.

Indicador: Número de acordos em trabalho. Assinatura de Acordos bilaterais (Croácia, Chipre, Bósnia e Herzegovina, Geórgia, Macedónia do Norte, Sérvia, Reino Unido, Argélia, India, Qatar e Bélgica).

DEPARTAMENTO DE GESTÃO DA INFORMAÇÃO CLASSIFICADA E CRIPTOGRAFIA (GICC)

O Departamento de Gestão da Informação Classificada e Criptografia tem por missão apoiar a Autoridade Nacional de Segurança garantindo que a gestão do ciclo de vida da IC 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, garantindo que a administração e distribuição de material criptográfico se efetue por canais separados.

OBJETIVOS OPERACIONAIS

GICC_PI102- Otimizar a utilização das instalações do "Sub-Registo as a Service".

Indicador 1: Conclusão das melhorias nas infraestruturas do "Sub-Registo as a service".

Meta: 31 de dezembro

Indicador 2: Inicial Operability Capability (IOC).

Meta: 31 de dezembro

GICC_P102- Operacionalizar e certificar o Sistema de Segurança Eletrónica da Informação Classificada (eSEIF).

Indicador 1: Operacionalizar software (SW) em órgãos de segurança.

Meta: 6 entidades.

Indicador 2: Processo de certificação do eSEIF.

Meta: 50% do processo de certificação.

GICC_P103- Implementar novas funcionalidades e melhorias (eSEIF 2.0 e eSEIF Light).

Indicador: Percentagem de desenvolvimento do novo software que incluirão novas funcionalidades e melhorias.

Meta: 50%. do desenvolvimento.

GICC_P104- Participação no projeto DISCRETION, visando a disponibilização de uma solução Criptográfica Nacional a 150 autoridades públicas até 2026.

Indicador 1: Data de aprovação do protocolo nacional para o financiamento do projeto entre as 4 entidades da administração central do Estado (GNS/MDN/EMGFA/DEIMOS).

Meta: 30 de abril

Indicador 2: Desenho da rede Software Defined Network (SDN) com capacidade *Quantum Key Distribution* (QKD) e desenho da máquina de cifra com QKD (Work Package 5).

Meta: 30 de outubro

Indicador 3: Data de aprovação de um Memorando pelos 4 países participantes no projeto.

Meta: 30 de abril

GICC_P105- Operacionalização da implementação da plataforma de Gestão de Material Cripto (SCRIPTO).

Indicador 1: Data da capacidade Inicial de Operação (IOC) no GNS.

Meta: 31 de dezembro

Indicador 2: Processo de certificação de segurança da plataforma SCRIPTO.

Meta: 31 de dezembro de 2025

GICC_P106 – Desenvolvimento evolutivo da máquina de cifra HSM-T2 para nova versão 2.1.

Indicador 1: Plano de industrialização para o fabrico de 100 unidades.

Meta: 30 de junho

INDICADORES DE ATIVIDADE

IA107 – Operacionalização do HSMT 2.0.

Indicador 1: Data de entrega dos HSMT 2.0 aos utilizadores finais.

Meta: 30 de abril

IA108 – Distribuição de material de cifra por canais separados.

Indicador: Assegurar a receção presencial de material criptográfico em Portugal e no estrangeiro (Rota, Espanha).

Meta: 12 deslocações.

IA109 – Garantir o apoio nos processos de credenciação de pessoas singulares via CRESO.

Indicador 1: Número de processos de credenciação de pessoas singulares GNS/CNCS e cumprimento do preconizado nas Normas Técnicas relativamente a esta área.

Meta: 40 processos e elaboração de listas semestrais.

Indicador 2: Número de credenciações de pessoas singulares de entidades públicas.

Meta: 200 processos e elaboração de listas semestrais.

IA110- Garantir o apoio técnico rede SEIF.

Indicador: Número de ações de apoio aos órgãos de segurança da Estrutura Nacional de Segurança da Informação Classificada (ENSIC) na resolução de anomalias e na manutenção preventiva do SEIF.

Meta: 1200 ações de apoio.

IA111 – Garantir o apoio nos processos de gestão do ciclo de vida da Informação Classificada.

Indicador: Número de entidades públicas apoiadas.

Meta: 5.

IA112 – Controlar o cumprimento das normas técnicas pelos Sub-Registos da ENSIC.

Indicador: Registar e controlar o envio de todos os relatórios periódicos pelos Sub-Registos.

Meta: 108 relatórios.

IA 113 – Apoio interno à gestão de ciclo de vida da IC.

Indicador: Número de documentos classificados registados e destruídos.

Meta 1: 1000 registos de documentos.Meta 2: 500 processos de destruição de documentos.

IA 114 - Distribuição de IC.

Indicador: Número de documentos distribuídos em formato físico e digital aos órgãos de segurança.

Meta 1: 600 documentos em formato papel.

Meta 2: 1000 em formato digital.

DEPARTAMENTO DE SEGURANÇA DIGITAL, TECNOLÓGICA E DE INFRAESTRUTURAS (SDTI)

O Departamento 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.

Áreas de competência do Departamento

- Segurança Tecnológica
- Segurança das Infraestruturas
- Segurança do Espaço
- Serviços de Confiança

Segurança Tecnológica

Compete à Segurança Tecnológica, avaliar, certificar e acreditar 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 informação classificada, assim como, proceder à realização de limpezas eletrónicas em áreas sensíveis onde seja tratada informação com necessidades especiais de segurança.

Segurança das Infraestruturas

Contribui para a Acreditação/Certificação das infraestruturas, dos sistemas ou equipamentos de segurança que conferem proteção física aos locais ou SIC que processem, arquivem ou transmitam informação classificada, competindo-lhe ainda colaborar nas inspeções periódicas aos órgãos de segurança sob responsabilidade portuguesa, no território nacional e no estrangeiro, detentores de informação classificada.

Segurança do Espaço

Atua como autoridade responsável pela componente codificada do Sistema GALILEO, credenciação dos pontos de contacto nacionais no âmbito da sua componente de segurança e efetuar a gestão de chaves de cifra aquando da respetiva operação.

Serviços de Confiança

Apoiam o desenvolvimento das atividades da Entidade Supervisora dos Sistemas de Identificação Eletrónica (eID) nacionais, de Entidade Supervisora dos prestadores de serviços de confiança e como de Entidade Gestora das Listas de Confiança no âmbito do Regulamento (UE) n.º 910/2014, do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno, mais conhecido por regulamento eIDAS, transposto para a Legislação nacional pelo DL 12/2021 de 9fev, bem como no quadro do regime jurídico dos documentos eletrónicos e da assinatura eletrónica e para os efeitos nele previsto; (DL 136/2017 Artº2.3.j), e ainda apoiar no desenvolvimento das atividades da Autoridade Credenciadora no âmbito da Lei n.º 96/2015, de 17 de agosto, que regula a disponibilização e a utilização das plataformas eletrónicas de contratação pública; (DL 136/2017 Artº2.3.m).

A atividade do SDTI para 2024 traduz-se assim nos seguintes conjuntos de objetivos operacionais e atividades correntes:

OBJETIVOS OPERACIONAIS

SDTI_P107- Implementar o Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada, desenvolvendo parcerias com entidades de referência.

Indicador 1: Promulgar o Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada, através de diploma legal.

Meta: 30 de março

Indicador 2: Implementar a Comissão Técnica com vista a operacionalizar a utilização do Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada.

Meta: 30 de março

Indicador 3: Realizar ações de informação e difusão do Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada.

Meta: 30 de setembro

Indicador 4: Implementar Laboratório TEMPEST em parceria com o Centro Laboratorial e Normalização (CLN) da ANACOM.

Meta: 30 de agosto

SDTI_P108- Robustecer a capacidade de contramedidas eletrónicas através do alargamento ao domínio acústico e desenvolvimento do manual de procedimentos em conjunto com o reforço da capacidade de acreditação e auditoria de sistemas de informação classificada.

Indicador 1: Apresentação do manual de procedimentos relativos ao planeamento e desenvolvimento de operações de limpeza eletrónica.

Meta: 30 de maio

Indicador 2: Prazo para atualização de aplicação de avaliação de Zoning de acordo com o Modelo Nacional de Zona (NT - B03)

Meta: 30 de junho

Indicador 3: Prazo para manifestação de necessidades para aquisição de contramedidas eletrónicas para o domínio raio-x e jammers com inclusão de frequências 5G.

Meta: 30 de novembro

Indicador 4: Participação/realização de **duas** ações de partilha de conhecimento pratico e teórico, no âmbito da utilização de contramedidas eletrónicas, em parceria com entidades nacionais e estrangeiras.

Meta: 30 de dezembro

SDTI_P109- Organizar, difundir e promover a adoção do processo de Acreditação de Segurança de Sistemas de Informação e de Comunicação (SIC) habilitados a processar Informação Classificada, pelas organizações públicas e privadas.

Indicador 1: Criação de formulários modelo para instrução de processo de Acreditação de Segurança de Sistemas de Informação e de Comunicação (SIC) habilitados a processar Informação Classificada.

Meta: 31 de março

Indicador 2: Definição de perfil de avaliação técnico baseado em requisitos mínimos para Sistemas de Informação e de Comunicação (SIC) sujeitos a acreditação.

Meta: 31 de março

Indicador 3: Atualização de ferramentas de acreditação e de auditoria de sistemas de informação classificada.

Meta: 30 de junho

Indicador 4: Apresentação de Norma Técnica referente à condução de auditorias de segurança conducentes a processos de acreditação de segurança da informação, no âmbito da informação classificada.

Meta: 30 de setembro

SDTI_P110 - Edificação do Centro de Operações do Espaço de forma a permitir a implementação da capacidade de comunicações e posicionamento satélite seguras.

Indicador 1: Formação de 2 operadores e um técnico de informática da CPA.

Meta: 31 de março

Indicador 2: Apetrechamento da sala de operações com a *Sina Mission Network*.

Meta: 30 de maio

Indicador 3: Edificação da componente Govsatcom – fase 1 (instalação da componente RUE).

Meta: 30 de novembro

Indicador 4: Edificação da componente Govsatcom – fase 2 (instalação da componente SUE) condicionada a decisão superior sobre as instalações do GNS.

Meta: 31 de dezembro - 20% (correspondente à adjudicação da edificação e tempestização da sala do Govsatcom).

SDTI_P111 - Certificar e implementar um modelo de preservação digital de informação com requisitos especiais de segurança, referentes aos Processos de Credenciação.

Indicador 1: Desenvolvimento aplicacional do Interface gráfico e de gestão base de dados.

Meta: 31 de agosto

Indicador 2: Certificação do Software aplicacional.

Meta: 29 de dezembro

Indicador 3: Entrega de 20.000 processos de credenciação por parte do GNS à INCM;

Meta: 29 de setembro

Indicador 4: Digitalização de 20.000 processos de credenciação.

Meta: 29 de dezembro

SDTI_P112- Implementar o acesso descentralizado a cidadãos ou empresas de registos públicos do GNS no âmbito da certificação de produtos e serviços recorrendo à framework EBSI/Blockchain.

Indicador: Realização de Prova de Conceito.

Meta: 31 de novembro

SDTI_P113- Prosseguir com a criação da framework para materialização da capacidade para o desempenho das funções de entidade supervisora e de entidade gestora das listas de confiança, definidas pelo Regulamento (UE) n.º 910/2014 (eIDAS)

Indicador 1: Apresentação de proposta de normativo que define as regras de notificação de incidentes de segurança no que concerne ao consignado no artigo 19.º do Regulamento eIDAS

Meta: 31 de março

Indicador 2: Apresentação de proposta de revisão do normativo relativo à Identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência

Meta: 29 de setembro

SDTI_P114- Desenvolvimento de Norma Técnica (NT) e atualização das Listas de Verificação (LV) de Segurança Física de Infraestruturas que garantem proteção à Informação Classificada (IC).

Indicador 1: Prazo para apresentação da proposta de Norma Técnica (NT).

Meta: 30 de junho

Indicador 2: Prazo para apresentação da proposta de atualização das Lista de Verificação (LV) no âmbito da Segurança Física de Infraestruturas.

Meta: 31 de março

INDICADORES DE ATIVIDADE

IA115- Número de Processos de Certificação concluídos de produtos/serviços habilitados a processar IC.

Referência: 7

IA116- Número de Processos de Acreditação concluídos de sistemas autorizados a processar IC.

Referência: 6

IA117- Número de avaliações de Zoning.

Referência: 8

IA118- Número de Limpezas Eletrónicas.

Referência: 3

IA119 - Elaborar os diversos processos de acreditação PRS das empresas nacionais;

Referência: 3

IA120 - Inspecionar os sites nacionais da área do espaço (EGNOS Lisboa, EGNOS Madeira, SST) e elaborar os respetivos processos de acreditação;

Indicador: 3

IA121 - Criação/participação de novos processos transformacionais no âmbito da eID e Serviços de Confiança.

Referência: 1

IA122 - Pedidos de esclarecimentos gerais s/ TSP, Plataformas, outras (reuniões e helpdesk).

Referência: 42

IA123 - Pareceres enquadrados (Âmbito no Regulamento eIDAS, PECP, outros).

Referência: 5

IA124 - Auditorias/inspeção TSP (Regulamento eIDAS).

Referência: 3

IA125 - Atualização da TSL (Trusted List).

Referência: 5

IA126 - Credenciação e/ou renovação da credenciação de auditores de segurança.

Referência: 2

IA127 - Elaboração de Relatórios e Pareceres em Segurança Física no âmbito da Acreditação/Certificação de infraestruturas, dos sistemas ou equipamentos de segurança que conferem proteção física aos locais ou SIC que processem, arquivem ou transmitam informação classificada.

Referência: 10

Nota: As Referências são baseadas nos valores atingidos durante o ano de 2023

DEPARTAMENTO DE CREDENCIAÇÃO

O Departamento de Credenciação 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 organismos, onde seja administrada informação classificada ou que necessitem de desenvolver atividades especifica que, nos termos da lei, envolvam a administração dessa informação.

Para o corrente ano, entendemos que a atribuição de credenciações, a resposta a pedidos de investigação de segurança por parte de entidades nacionais de segurança homólogas e de outras organizações de que Portugal faz parte, o aumento de entidades a colaborar no processo de investigação de segurança, e a participação em representação do GNS nos fóruns onde a segurança industrial e a segurança de pessoal são discutidas, nomeadamente nos Grupos de Trabalho *Multinational Industrial Security Working Group* (MISWG), AC/35-D(2021)0001 (SP) (INV) - *Capability Team*, Security Scrutiny Group como National Security Expert nos programas Digital Europe, Horizon Europe e European Defense Fund e *EEAS Expert meeting on Personnel Security Clearance* da EU, concorrerão para atingir os objetivos operacionais definidos para 2024.

OBJETIVOS OPERACIONAIS

DC_P301- Estabelecer protocolos com Entidades Nacionais que podem colaborar nos processos de investigação de segurança a pessoas coletivas e pessoas singulares.

Indicador: Número de novas entidades a participar no processo de investigação de segurança.

Meta: 2

INDICADORES DE ATIVIDADE

IA128- Reuniões plenárias com os encarregados de segurança das empresas credenciadas.

Indicador: Número de reuniões.

Meta: 2 (uma por semestre).

IA129 – Reunião com Entidades de *Vetting*

Indicador: Número de reuniões

Meta: 1

IA130 – Credenciações e investigações de segurança em 2024.

Indicador 1: Rácio de credenciações de segurança de pessoas singulares solicitadas/emitidas.

Indicador 2: Rácio de credenciações de segurança pessoas coletivas solicitadas/emitidas.

Indicador 3: Rácio de pedidos de *Vetting* (ANS e EU) solicitados/emitidos.

IA131 – Número de Request For Visit (RfV), FSCIS e PSCIS.

Indicador 1: Número de RfV e FSCIS processados.

Indicador 2: Número de PSCIS processados.

SERVIÇO DE INFORMÁTICA, REDES E COMUNICAÇÕES (IRC)

A 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.

OBJETIVOS OPERACIONAIS

IRC_P115- Implementação do Multi Factor Authentication (MFA).

Indicador: Implementação do Final Operational Capability (FOC).

Meta: 31 de maio.

IRC_P116- Implementação do Dual Boot.

Indicador: Implementação do FOC.

Meta: 31 de maio

IRC_P117- Implementação da 1ª fase do Low Level da Rede Classificada ÉGIDE – grupo criptografia dos segmentos High, Low Level e capilaridade eSEIF, CORE, Switching e Data Diodos.

Meta: 31 de dezembro

Meta: 25%.

Risco: Demora na entrega de equipamentos.

IRC_PI103- Implementação do “Disaster Recovery”.

Indicador: Data para alcançar a Inicial Operability Capability (IOC).

Meta: 31 de dezembro

Risco: capacidade de resposta do EMGFA.

IRC_PI104- Atualização de funcionalidades na Gestão Documental

Indicador: Data para Interoperabilidade da gestão documental com outros Organismos Públicos.

Meta: 31 de março. Depende da AMA.

INDICADORES DE ATIVIDADE

IA127- Tickets.

Indicador 1: Número de tickets.

Indicador 2: Número de tickets fechados.

Indicador 3: Tempo de resolução.

IA128 – Incidentes.

Indicador 1: Número de incidentes.

Indicador 2: Número de incidentes fechados.

Indicador 3: Tempo de resolução.

IA129 –Incidentes analisados manualmente.

Indicador 1: Número de incidentes.

Indicador 2: Número de incidentes fechados.

Indicador 3: Tempo de resolução.

IA130 – Apoios ao CRESO.

Indicador 1: Número de apoios.

Indicador 2: Número de apoios fechados.

Indicador 3: Tempo de resolução.

IA131 – Apoios SEIF/eSEIF.

Indicador 1: Número de incidentes.

Indicador 2: Número de incidentes fechados.

Indicador 3: Tempo de resolução.

NÚCLEO DE APOIO À DIREÇÃO (NAD)

É um núcleo multidisciplinar que tem como propósito apoiar a Direção na tomada de decisão.
Os objetivos operacionais deste ano são os que se identificam.

OBJETIVOS OPERACIONAIS

NAD_G202 – **OP2** Desenvolvimento de novas funcionalidades e melhorias do sistema CRESO (CRESO+) **(Objetivo operacional do QUAR 2024)**

Indicador: Taxa de execução da implementação das novas funcionalidades.

Meta: 80%

NAD_G203 – **OP5** Promover a motivação das pessoas trabalhadoras do GNS/CNCS e melhorar a satisfação dos seus clientes (Nº de atividades) **(Objetivo operacional do QUAR 2024 – Relevante)**.

Indicador1: Número de atividades de team building realizadas pelas pessoas trabalhadoras do GNS/CNCS.

Meta: 3.

Indicador2: Grau de satisfação das pessoas trabalhadoras do GNS/CNCS e dos respetivos clientes.

Meta: 70%

NAD_G205 – Lançamento do processo concursal para a elaboração do Projeto de Arquitetura e de especialidades para a requalificação e habilitação das novas instalações do GNS/CNCS.

Indicador: Data de lançamento do Procedimento Concursal.

Meta: 31 de março

NAD_G208 – Melhoria dos Serviços - Revisão do Manual de acolhimento.

Indicador: Data

Meta: 30 de setembro

SERVIÇO DO OFICIAL DE SEGURANÇA (OF SEG)

O Oficial de Segurança é responsável, perante o Diretor-geral, por gerir, manter e operar os diversos sistemas de segurança física existentes no GNS e no CNCS, tendo em vista o garante da:

Gestão dos recursos humanos afetos à segurança, nomeadamente os que trabalham na Portaria;

Segurança física das instalações em termos de controlo de acessos, videovigilância dos espaços e áreas mais sensíveis e a deteção da intrusão;

Manutenção e funcionamento dos sistemas de deteção e combate a incêndios;

Gestão dos lugares de estacionamento de viaturas de serviço e de colaboradores;

Elaboração, alteração e revisão dos Planos de segurança e de Emergência;

Coordenação, planeamento e condução dos exercícios e simulacros de segurança determinados pelo Diretor-geral.

OBJETIVOS OPERACIONAIS

NAD_G206 – Reforçar a Segurança Física das instalações.

Indicador 1: Resolução de anomalias no Sistema Automático de Deteção de Incêndios (SADI).

Meta: 31 de outubro

Indicador 2: Incremento da capacidade de controlo de presenças, através da aquisição e instalação de equipamentos de nova geração em pontos-chave do complexo. Visa aliar um processo de integração gradual de redes com a necessidade de rapidamente analisar o número e localização de efetivos para efeitos de evacuação.

Meta: 31 de outubro

Indicador 3: Expansão da cobertura do Sistema de Videovigilância no GNS/CNCS.

Meta: 31 de outubro

NAD_G207 – Reforço do treino de Segurança.

Indicador: Realização de dois exercícios de evacuação.

Meta: 20 de dezembro

CENTRO NACIONAL DE CIBERSEGURANÇA

O conceito de Cibersegurança, ao longo dos tempos, até motivado pela própria noção de transformação digital, tem sido alvo de diversas interpretações. Se pode ser entendido como o conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças a que estão expostos, tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, pode, por outro lado, ser definido como o sentimento de segurança percecionado pelas pessoas quando usam a Internet e as tecnologias digitais.

É precisamente com um foco neste contexto de interação em segurança, tanta quanto possível, de pessoas, processos e tecnologias, que o Centro Nacional de Cibersegurança (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.

DEPARTAMENTO DE DESENVOLVIMENTO E INOVAÇÃO (DDI)

O Departamento de Desenvolvimento e Inovação (DDI) tem como objetivo principal contribuir ativamente para a capacitação e promoção do capital humano, através de programas de sensibilização e disseminação de boas práticas dirigidos à população em geral, mas também a públicos específicos, como adultos mais velhos e jovens, bem como mediante formação e treino avançados para profissionais especialistas. A tomada de decisão informada, a produção de conhecimento situacional e a influência positiva sobre as políticas públicas na área da cibersegurança são propósitos do DDI. Por fim, e de forma transversal, o DDI aplica estratégias de comunicação que procuram fomentar o envolvimento da comunidade de interesse e a criação de grandes eventos, distribuídos geograficamente, que contribuam para o incremento da literacia e da formação de redes de colaboração entre partes interessadas.

Sensibilização, Formação e Treino (SFT)

A área da Sensibilização, Formação e Treino tem como objetivo desenvolver e implementar programas de educação e consciencialização de cidadãos e colaboradores de organizações, sobre práticas e comportamentos seguros no uso de tecnologia, na proteção de informação sensível e na resposta aos desafios da cibersegurança.

No domínio da sensibilização, em 2024, o Centro Internet Segura (CIS) dará continuidade ao trabalho desenvolvido pelo consórcio e pelo CNCS, assegurando a manutenção das iniciativas e atividades de sensibilização e treino, nomeadamente através das seguintes atividades: MOOCs; parceria com o Instituto para os Comportamentos Aditivos (ICAD) na dinamização do jogo digital "Eu e os Outros"; implementação do Roadshow ZigZaga da Net e do Roadshow CIS LAB; dinamização do Dia da Internet Mais Segura; recursos digitais que darão robustez ao CIS - Cybersecurity LAB; e a resposta a solicitações de sessões de sensibilização através do canal público existente no website do CIS.

O CIS Digital Camp é um programa intensivo, de uma semana, dirigido a jovens do ensino secundário e cujo objetivo é fornecer ferramentas e conhecimentos necessários para navegar no ciberespaço de forma responsável, segura e saudável. No âmbito dos materiais do CIS - Cybersecurity LAB, serão criados os seguintes recursos: um recurso sobre desinformação destinado aos jovens - "Fake it to make it"; um recurso digital dirigido aos adultos mais velhos; e a adapatação digital do "ZigZaga na Net" destinado a crianças. De referir, ainda, que será desenvolvido um livro de pintar enquadrado com frases alusivas à literacia digital, para crianças do ensino pré-escolar, com o objetivo de, por um lado, influenciar os pais, avós e comunidade escolar e, por outro, para que as crianças percebam o seu papel como agentes de mudança e reconheçam os efeitos das suas atitudes no meio digital. Ainda no domínio da sensibilização, os quatro cursos de e-learning (MOOCs) continuarão a servir como instrumento central de sensibilização dos cidadãos em matéria de cibersegurança e será ainda implementado um novo curso – Cidadão Ciberinclusivo, cujo objetivo é capacitar, no âmbito da ciber-higiene, os cidadãos com necessidades educativas especiais. Serão ainda

desenvolvidos conteúdos de boas práticas que contribuirão para a sensibilização e robustecimento dos comportamentos de cibersegurança dos cidadãos em geral.

A C-Academy - programa de formação avançado em cibersegurança - continuará a ser o instrumento que irá formar e requalificar quadros especializados em cibersegurança nas Empresas e na Administração Pública. Neste sentido, continuar-se-á, através da parceria com as instituições de ensino superior, a apostar no desenvolvimento de conteúdos para os cursos e na aplicação geográfica dos mesmos.

O Cybersecurity Challenge PT, por sua vez, é uma atividade que se enquadra num programa de formação e treino abrangente, cujo objetivo passa por promover a cibersegurança e a identificação de talentos do ensino secundário e superior. Neste âmbito, pretende-se dinamizar seis iniciativas de divulgação e competição de CTF - Capture the flag, desenvolvendo-se três teasers para jovens do ensino secundário e três CTF para jovens universitários, tendo como objetivo identificar e selecionar os membros que irão jogar e representar o país nas competições internacionais, em particular no European Cybersecurity Challenge 2024.

Transversalmente à área da Sensibilização, Formação e Treino pretende-se estabelecer parcerias com Entidades Intermunicipais e instituições educativas para integrar a cibersegurança nos currículos e promover a consciencialização desde cedo. Isso inclui o desenvolvimento de materiais educativos específicos e a realização de programas de sensibilização em escolas e universidades.

Conhecimento Situacional (CS)

O Observatório de Cibersegurança visa observar o fenómeno da cibersegurança em Portugal, nas suas mais variadas componentes, de modo a informar as partes interessadas e a suportar a definição de políticas públicas. Com uma visão multidisciplinar, o Observatório de Cibersegurança sistematiza informação disponível ou promove a sua recolha nos domínios da Sociedade, Economia, Políticas Públicas, Ética e Direito, Riscos e Conflitos, bem como Inovação e Tecnologias Futuras.

Neste âmbito, em termos de estratégia, 2024 será um ano dedicado a tornar o trabalho em curso e regular mais consistente, mas adicionando alguns produtos considerados relevantes. Neste sentido, serão publicados os cinco boletins habituais, bem como os Relatórios sobre a Cibersegurança em Portugal relativos aos temas Sociedade e Riscos e Conflitos. Serão ainda terminados os trabalhos relativos aos sete relatórios setoriais sobre os operadores de serviços essenciais.

Como novos trabalhos, serão melhorados os conteúdos em Power BI publicados no website do CNCS e alargadas as temáticas aí tratadas a todas as áreas do Observatório, bem como será subcontratado um Estudo Sobre o Ensino da Cibersegurança no Ensino Obrigatório em Portugal.

Comunicação e Imagem (C&I)

A área da Comunicação e Imagem tem como objetivo gerir e promover a imagem do CNCS através da definição de estratégias que permitam construir, fortalecer e proteger a reputação da Instituição. Na sua área de ação integram-se os eventos institucionais, a relação com os media, a comunicação interna e externa, a comunicação estratégica e o design gráfico.

No âmbito da comunicação externa, em particular na relação com os media, vão continuar a ser fortalecidas relações de confiança com os media, nomeadamente através da articulação de respostas aos pedidos dos órgãos de comunicação social, bem como de ações de esclarecimento, formações e difusão de comunicados

à imprensa. Esta atividade é alvo de monitorização constante, com destaque para os cadernos de Imprensa das diversas ações e atividades desenvolvidas pelo CNCS.

O portfólio de serviços vai continuar a ser divulgado com base em planos de comunicação e mensagens-chave, que visam impactar e atrair os partes interessadas. Continuará a ser produzido conteúdo diferenciado para os diferentes canais de comunicação, tais como: redes sociais; sites institucionais (CNCS e CIS); podcast "Comunicar Cibersegurança"; webinar "Cibertemas"; e os canais internos e externos de parceiros. Haverá uma aposta em novas tipologias de conteúdos, como desenvolvimento de infografias, vídeos, casos de sucesso ou role model partilhando experiências, desafios ou concursos, entre outros, criando engagement com as várias personas.

A C-DAYS vai continuar a proporcionar um ambiente de partilha de conhecimento, visões e práticas de cibersegurança, numa perspetiva estratégica, operacional e técnica, contribuindo para uma cultura nacional de cibersegurança. Em 2024, a cidade de Coimbra é o local escolhido para reunir líderes empresariais, especialistas e académicos com o objetivo de discutir experiências e caminhos a adotar no crescimento da maturidade em cibersegurança. Haverá ainda uma aposta na "C-Days Parceiros", com coorganização de organismos regionais e geograficamente dispersos pelo país.

Relativamente à comunicação interna pretende-se garantir que os colaboradores são informados sobre os projetos e atividades e envolvidos na vida do CNCS permitindo que sejam os primeiros embaixadores do CNCS junto dos cidadãos, organizações e parceiros. Neste sentido, continuar-se-á a dinamizar a rúbrica mensal "O que se passa no CNCS" e serão partilhadas informações sobre reuniões e eventos via e-mails corporativos.

No que diz respeito à imagem e identidade corporativa continuar-se-á a gerir a marca de vários projetos e, em particular, do CNCS, garantindo a consistência e transmitindo os valores e a personalidade da organização. Neste sentido, internamente, vai ser desenvolvida uma estratégia de acompanhamento sobre o uso correto da identidade visual e dos templates associados, de forma a garantir a sua harmonização. Haverá ainda uma aposta no desenvolvimento de campanhas de publicidade com o objetivo de reforçar a missão do CNCS.

No âmbito da gestão de crise, vão ser desenvolvidos planos de comunicação de crise para lidar com situações que possam afetar a reputação do CNCS.

De referir ainda que a Comunicação e Imagem vai continuar a ser uma área transversal ao CNCS, apoiando e potenciando os vários departamentos.

OBJETIVOS OPERACIONAIS

DDI_PI105 – Dinamizar do Bootcamp CIS Digital Camp.

Indicador: Realização do Bootcamp.

Meta: 31 de agosto

DDI_P126 – Desenvolver conteúdos em Power BI (PBI) em todas as áreas do Observatório no site do CNCS.

Indicador: Número de áreas com conteúdos do Observatório em PBI, publicadas no site CNCS.

Meta: 6

DDI_PI107 – Avaliar a conferência C-DAYS2024.

Indicador: Entrega do relatório da conferência.

Meta: 30 de outubro

DEPARTAMENTO DE CAPACITAÇÃO TÉCNICA E ORGANIZACIONAL (DCTO)

O Departamento de Capacitação Técnica e Organizacional (DCTO) tem como objetivo informar e capacitar as organizações com as melhores práticas, através de um conjunto de atividades, ferramentas e serviços desenvolvidos 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 o apoio a organizações através da produção de documentação ou referenciais, sob a forma de boas práticas, guias e recomendações técnicas, prestando também o respetivo suporte e acompanhamento técnico em termos de operacionalização, visando aumentar a maturidade e resiliência organizacional em termos de cibersegurança.

Capacidades nas Organizações (CO)

Ao nível do desenvolvimento de capacidades nas organizações, no ano de 2024 será dada prioridade à operacionalização dos principais projetos de capacitação.

Neste âmbito, a C-Network surge como uma iniciativa inovadora e transformadora no apoio às entidades, com especial atenção às PMEs, Administração Pública local e entidades abrangidas pelo RJSC. Em 2024, e na sequência da instalação e operacionalização dos seus sete centros de competências, a C-Network prestará apoio e aconselhamento às entidades a que eles recorram, focando atividades relacionadas com segurança de informação, processos de transformação digital, apoio à procura de financiamento e de capacitação, entre outras em que se demonstre a necessidade de apoiar as referidas entidades em competências relacionadas com a cibersegurança. A C-Network pretende ainda ser o ponto de ligação entre os vários projetos e atividades do CNCS atuando em regime de proximidade com os vários agentes locais.

Também o polo de inovação digital C-HUB: Cybersecurity DIH (C-HUB), foi criado para fomentar a introdução da inovação e cibersegurança nos processos de transformação digital, com o intuito de apoiar as PMEs e entidades da Administração Pública no seu caminho para a ciber-resiliência. Consistindo num consórcio de sete entidades e numa lógica de “Testar antes de investir”, o C-HUB fornecerá atividades de experimentação e demonstração, prototipagem, certificação e transferência de tecnologia em cibersegurança, assumindo-se deste modo como uma referência na implementação de processos de transformação digital. No ano de 2024, o C-HUB estará focado na implementação operacional das atividades previstas em sede de candidatura visando cumprir a estratégia, missão e objetivos.

O CNCS foi constituído como Centro Nacional de Coordenação em Cibersegurança (NCC-PT), na sequência do regulamento 2021/887 efetivado pelo despacho conjunto n.º 11491/2022 dos ministérios da Ciência e Tecnologia, Economia e Secretaria de Estado para a Digitalização e da Modernização Administrativa. O NCC-PT está integrado no âmbito da rede de centros nacionais de coordenação para a cibersegurança no espaço Europeu e em estreito alinhamento com a missão e atividades delegadas pelo Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC). O NCC-PT operacionaliza a sua atividade através do consórcio formado pela Agência Nacional de Inovação (ANI) e Fundação para a Ciência e a Tecnologia (FCT), num modelo de responsabilidades partilhadas em termos de

atividades de âmbito nacional, conforme despacho que efetiva a atribuição do NCC-PT ao CNCS, funcionando os restantes membros como entidades de suporte à missão e atividades. Na sequência do financiamento europeu atribuído ao NCC-PT interessa agora garantir a sua operacionalização e prossecução das suas principais atribuições. Nesse sentido, caberá ao CNCS assegurar a coordenação, monitorização e acompanhamento das ações e decisões tomadas no âmbito do consórcio; funcionar como ligação entre o NCC-PT, o ECCC, e a Comissão; a gestão e execução das subvenções atribuídas ao NCC-PT; a criação, registo, manutenção e apoio à comunidade nacional de cibersegurança; a participação nas atividades de cooperação solicitadas ao NCC-PT pela comissão, ECCC e ENISA no âmbito da rede europeia de NCCs em alinhamento acordo com as decisões e estratégias definidas para o NCC-PT.

O DCTO irá promover, em 2024, o planeamento, organização e a execução de dois Exercícios de Cibersegurança, atividade que visa promover o treino e a capacitação de entidades para a prevenção e reação a incidentes de cibersegurança. Já no primeiro trimestre, e no âmbito de outras ações para melhorar a cibersegurança e resiliência dos atos eleitorais de 2024, será organizado um Exercício com o objetivo de treinar e capacitar as entidades que desempenham um papel significativo na realização dos próximos atos eleitorais (eleições para o parlamento europeu e legislativas nacionais). À semelhança dos anos anteriores, será também assegurada a organização do Exercício Nacional de Cibersegurança (ExNCS) que decorrerá, tal como em 2022, no âmbito do planeamento e execução do exercício europeu CyberEurope 2024 e que será direcionado aos setores da energia, prestadores de serviços digitais e administração pública. Adicionalmente, o DCTO irá apoiar as congéneres de Moçambique e Cabo Verde na organização do seu primeiro exercício de Cibersegurança, igualmente focado no setor da energia.

Redes de Colaboração (RC)

No que diz respeito às redes de colaboração nas quais o CNCS se encontra envolvido, destaca-se a promoção das atividades de cooperação e troca de experiências no âmbito dos vários ISACs, a dinamização das atividades da Aliança para a Cibersegurança e a organização de sessões de partilha de conhecimento (fóruns) no âmbito da administração pública central e local.

A criação e dinamização de Centros de Análise e Partilha de Informação (ISACs) serve o objetivo de fomentar o desenvolvimento de comunidades de parceiros no âmbito dos setores mais críticos ou sensíveis. Através da promoção da confiança e debate entre pares, em 2024, pretende-se estimular e acompanhar continuamente os ISACS já criados (setores das águas, energia, media, portos marítimos, retalho e distribuição, saúde e região autónoma dos açores) e, por outro lado, proporcionar a operacionalização de novos ISACs setoriais e regionais. Adicionalmente, e numa perspetiva de garantir o necessário suporte técnico à dinamização e aproximação destas comunidades, será disponibilizada uma plataforma de comunicação a estas comunidades de Cibersegurança.

Ainda no âmbito da dinamização das redes de colaboração, o DCTO apoiará a Aliança para a Cibersegurança na execução do seu plano de atividades. Em 2024, a Aliança para a Cibersegurança, que conta atualmente com treze membros, desenvolverá um conjunto de novas atividades e dará seguimento a alguns projetos de relevo iniciados em 2023 (por exemplo, a conclusão da revisão dos requisitos que caracterizam o selo de maturidade digital).

Com o objetivo de fomentar a colaboração e partilha de boas práticas entre as suas entidades, o DCTO continuará a assegurar a organização das duas edições anuais do fórum de Cibersegurança da Administração Pública. Por outro lado, e com o objetivo de aproximar e consolidar a rede colaboração potenciada pelo ExNCS 2023, pretende-se organizar um ou dois eventos anuais, igualmente sob a forma de fórum de partilha,

que envolvam as principais entidades da administração pública local (entidades intermunicipais e autarquias).

Guias e Normativos Técnicos (GNT)

Cumpridos quatro anos desde a sua publicação, torna-se necessário adaptar o Quadro Nacional de Referência em Cibersegurança (QNRCS) e referenciais/ferramentas associadas (Quadro de Avaliação de Capacidades de Cibersegurança e CiberCheckUp), considerando a evolução entretanto registada. Nesse sentido, em 2024 será desenvolvida e disponibilizada a segunda versão do QNRCS e adaptados os seus produtos complementares.

No âmbito da disponibilização do Selo Digital de Cibersegurança e da importância que lhe é reconhecida como instrumento de capacitação em cibersegurança para organizações de pequena e média dimensão, será produzido e disponibilizado um guia para melhor compreensão e apoio à implementação dos seus requisitos.

Tendo em conta a relevância atribuída à gestão de riscos em cibersegurança, e na sequência da publicação do guia e ferramenta de suporte, o DCTO promoverá e acompanhará a sua adoção e implementação num conjunto de entidades. Esta atividade permitirá verificar a adequabilidade da ferramenta Monarc, e recolher os dados necessários para a sua eventual adaptação e evolução.

OBJETIVOS OPERACIONAIS

DCTO_PI108 – Instalação dos Centros de Competência (Nº de Centros de Competência instalados)

Indicador: Instalações físicas disponíveis nas regiões NUT II.

Meta: 5.

DCTO_PI109 – Disseminar o National Coordination Centre (NCC-PT**)**

Indicador: Número de eventos de disseminação realizados.

Meta: 3.

DCTO_PI112 – Avaliar o exercício nacional e europeu CyberEurope24**.**

Indicador: Entrega do relatório do exercício nacional e europeu.

Meta: 31 de dezembro.

DEPARTAMENTO DE OPERAÇÕES (DO)

O Departamento 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.

Para o cumprimento da sua missão, o Departamento de Operações recorre a um conjunto de sistemas e processos de suporte que permitem o tratamento de observáveis e eventos a partir de fontes de informação externas e internas, o registo e gestão de incidentes de cibersegurança, a investigação e a análise forense sobre esses mesmos incidentes.

Neste âmbito são assegurados os seguintes serviços:

i. Gestão e coordenação a resposta a incidentes de cibersegurança no ciberespaço de interesse nacional (GCI);
ii. Deteção e prevenção de incidentes de cibersegurança no ciberespaço de interesse nacional (DPI);
iii. Produção do Quadro Situacional da Cibersegurança Nacional (QS);

Gestão e Coordenação de Incidentes (GCI)

É expetável que, tal como no ano transato, o número de incidentes reportados ao CERT.pt durante o ano de 2024 venha a subir de forma considerável.

De forma a suportar este incremento, melhorando simultaneamente a capacidade de resposta a incidentes, prevê-se a renovação total da sala de operações. Esta permitirá não só acomodar um maior número de operadores, mas fazê-lo em condições de maior conforto, garantindo ainda uma maior eficiência ergonómica do espaço. Ao mesmo tempo, serão instalados novos sistemas de monitorização, com interatividade melhorada, permitindo assim a eficaz visualização de todas as ferramentas ao dispor do Departamento.

Ao mesmo tempo persistirá o esforço de melhoramento e evolução do hardware e software dedicado a esta tarefa, procurando soluções que permitam a prestação de um melhor serviço à comunidade servida pela instituição.

A recolha de indicadores de comprometimento em redes e sistemas afetados por ataques informáticos é um importante vetor na obtenção de dados únicos que permitam efetuar ações preventivas em alvos semelhantes. Pretende-se capacitar o CERT.pt de meios de recolha, processamento e armazenamento de dados forenses avançados. Para tal o CERT.PT perseguirá um caminho de dotação contínua dos meios técnicos e humanos necessários ao cumprimento desse desígnio.

Deteção e Prevenção de Incidentes (DPI)

Melhorar a confiabilidade do acesso à Internet para todos os utilizadores na comunidade servida pelo CNCS é um objetivo ambicioso, mas ao qual o CERT.PT não deve furtar-se, dada a sua relevância para a melhoria contínua do patamar de cibersegurança nacional. Nesse sentido este Departamento propõe a criação e disponibilização à comunidade durante 2024, de um serviço DNS RPZ (Domain Name Service Response Policy Zones), contribuindo para o enriquecimento do arsenal de ferramentas de segurança à disposição das entidades nacionais.

Ao mesmo tempo e atendendo ao potencial do vasto conjunto de dados recolhidos e processados pelo CERT.PT afigura-se como pertinente a introdução de mecanismos de inteligência artificial, visando contribuir para uma melhor visibilidade sobre o panorama geral da cibersegurança através da criação de novos mecanismos de alerta e notificação.

Será ainda uma prioridade do CERT.PT para 2024 o melhoramento do mecanismo de gestão de vulnerabilidades MAGv através do reforço dos sistemas de alimentação de novas vulnerabilidades, mapeamento contínuo de infraestruturas digitais expostas e de alerta para vulnerabilidades críticas.

Quadro Situacional (QS)

No âmbito da produção de um Quadro Situacional da Cibersegurança Nacional, o PANORAMA incrementa a visibilidade sobre o conjunto de entidades de interesse que concorrem para a cibersegurança nacional.

Para este objetivo dar-se-á continuidade à caracterização das atividades de organismos (públicos ou privados).

Esta ferramenta, que permite ao CNCS ter visão global do estado do ciberespaço nacional, em tempo real num qualquer momento presente, continuará a ser desenvolvida durante o ano de 2024.

OBJETIVOS OPERACIONAIS

DO_P127 – Criar novas Normas Operacionais (Standard Operating Procedure - SOP)**.**

Indicador: Operacionalização no DO das novas SOP.

Meta: 30 de novembro.

DO_P128 – Disponibilização do DNS RPZ - Domain Name Service Response Policy Zones**.**

Indicador: Publicitação para a comunidade nos canais CNCS.

Meta: 31 de dezembro.

DO_PI111 – Elaborar procedimento de contratação da evolução do mecanismo de gestão de vulnerabilidades MAGv .

Indicador: Publicação do procedimento na ACINGov.

Meta: 30 de setembro.

DEPARTAMENTO DE REGULAÇÃO, SUPERVISÃO E CERTIFICAÇÃO (DRSC)

O Departamento 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 (RJSC), 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.

Para exercício da função de regulação o DRSC assegura a produção de referenciais técnicos e normativos em matéria de cibersegurança; a elaboração e aprovação de regulamentos nos casos previstos na lei e quando se mostrem indispensáveis ao exercício das suas atribuições, ou outras normas de caráter particular referidas a interesses, obrigações ou direitos das entidades ou atividades destinatárias da sua atividade; e a aprovação de instruções e a formulação de recomendações.

O DRSC zela pelo cumprimento das obrigações decorrentes dos normativos de cibersegurança, procedendo à sua monitorização, apoio às entidades abrangidas, supervisão, fiscalização e exercício das competências sancionatórias do CNCS.

O DRSC contempla ainda as áreas referentes às funções de Autoridade Nacional de Certificação da Cibersegurança atribuídas ao CNCS, conforme estabelecidas no Regulamento UE 2019/881 e do Decreto-Lei n.º 65/2021, de 30 de julho.

Dadas as atribuições enquanto Autoridade Nacional de Cibersegurança, o DRSC também atua no domínio do planeamento de emergência da cibersegurança.

O DRSC assegura as funções de CISO do GNS / CNCS e garante a prestação de uma gama de outras atividades permanentes, como a representação em fora internacional, o apoio à Tutela, a cooperação nacional e internacional e a participação em eventos ad hoc.

Regulação (RG)

Em 2024, prevê-se a continuação do trabalho de transposição e implementação da Diretiva NIS 2, que teve como primeiros resultados o estudo e avaliação de impacto da NIS 2 em Portugal e uma proposta inicial de transposição entregues em 2023. O DRSC procederá ao controlo e execução das obrigações internacionais de Portugal decorrentes da NIS 2.

Nos termos do n.º 1 do artigo 18.º e do n.º 7 do artigo 3.º do Decreto-Lei n.º 65/2021, de 30 de julho, prevê-se a publicação do Regulamento relativo à implementação do RJSC na Administração Pública. Findo o processo prévio de consulta pública, serão trabalhados os contributos recolhidos e elaborado um relatório público. Uma nova versão do Regulamento será então produzida, aperfeiçoada com os contributos relevantes, e submetida a aprovação para publicação.

A nível setorial, o CNCS procederá à necessária articulação com as entidades setoriais relevantes para a aplicação do Network Code on Cybersecurity aims to set a European standard for the cybersecurity of cross-border electricity flows, assim como do Cyber Resilience Act.

Associado ao trabalho de regulação, haverá um esforço de divulgação, sensibilização e prestação de informações às entidades abrangidas pelos normativos referidos.

O DRSC assegura o contributo nacional para a cooperação europeia em matéria de implementação harmonizada da Diretiva NIS 2 e outros normativos de cibersegurança, em sede do Grupo de Cooperação da Diretiva da Segurança das Redes e da Informação (NIS Cooperation Group). De destacar que o DRSC garante a liderança do Work Stream (WS) do setor da Saúde. Além disso, assegura a coliderança do Work Stream alusivo ao 5G/Telecomunicações e participa nos WS sobre Supervisão, sobre Eleições, on Digital Infrastructure and Providers (sendo que nestes dois últimos, o DRSC tem desenvolvido um trabalho de relevo), on Cybersecurity Risk Management Measures, on Cybersecurity Incident Reporting, sobre a Energia, on WhoIS Database, on Risk Evaluations and Scenarios, on Supply Chain Security e no Working Group on Aviation.

Supervisão (SV)

O DRSC continuará o projeto de desenho e conceção de processos de Supervisão do RJSC, com enfoque na NIS 2. Neste projeto, prevê-se o desenvolvimento dos processos com a entidade adjudicada, através da prestação de informações e de reuniões de controlo da conformidade e adequação dos trabalhos desenvolvidos. O projeto terá como entregáveis um estudo sobre os processos de supervisão da cibersegurança e a especificação de requisitos técnicos e funcionais para a escolha de uma ferramenta de apoio a adotar.

Uma atividade instrumental para a supervisão consistirá na Identificação e monitorização de entidades abrangidas pelo atual RJSC e pela NIS2. Assim, proceder-se-á à recolha de informação para identificação das

entidades abrangidas pelo Regulamento relativo à implementação do RJSC na Administração Pública, e pela NIS 2, tendo em vista a definição dos universos destes normativos.

Neste ano, iniciar-se-á a atividade de Supervisão do RJSC por meio de auditorias. Para esse fim, será inicialmente desenvolvida documentação de apoio à atividade de supervisão. Será também efetuado o recrutamento de recursos humanos para a constituição de uma bolsa de peritos qualificados para a execução de auditorias de cibersegurança, a quem será prestada formação específica, contribuindo para o cumprimento do contrato do PRR, que prevê a capacitação de auditores especializados.

Para exercício das competências sancionatórias no âmbito do RJSC, será compilado um acervo de documentação de apoio à atividade de instrução de processos de contraordenação, incluindo modelos de peças processuais e outros documentos administrativos, incluindo notificações de incumprimento e para restabelecimento da conformidade.

No decurso de 2024, serão efetuadas notificações de incumprimentos do RJSC reportados ao ano de 2023, de que resultará a respetiva abertura de inquéritos por incumprimentos.

Ainda como atividade a desenvolver no contexto da supervisão, ter-se-á em conta a implementação do Decreto-Lei n.º 116/2023, de 20 de dezembro, que transfere para o CNCS as competências de fiscalização e de instrução de contraordenações no âmbito do ECOMPENSA, sobretudo quanto à competência de fiscalização das plataformas eletrónicas.

Por último, como resultado do projeto de desenho e conceção de processos de Supervisão do RJSC, procurar-se-á dar início ao desenvolvimento de ferramentas de apoio à supervisão, nesta se incluindo a atividade em prol dos procedimentos contraordenacionais, de acordo com especificações técnicas que resultem do projeto.

Certificação (CTF)

Em 30 de julho de 2021, foi publicado o Decreto-Lei 65/2021 que designa o CNCS como Autoridade Nacional de Certificação da Cibersegurança (ANCS), incluindo para efeitos do disposto no Regulamento UE 2019/881, no âmbito do enquadramento europeu de certificação da cibersegurança, e possibilita a edificação de um quadro nacional de certificação da cibersegurança e sua governação pelo CNCS.

A nível nacional, será elaborado um esquema de certificação de empresas de serviços de cibersegurança, para responder à necessidade de constituição de um catálogo de prestadores nacionais de serviços de cibersegurança confiáveis, que cumpram com o conjunto de requisitos de serviço definidos pelo esquema e cujo desempenho seja alvo de avaliação e monitorização periódica.

Tendo o DRSC já publicado o Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança, e facilitado a elaboração e publicação do respetivo esquema de acreditação, será estimulada a acreditação de organismos para o exercício de atividades de certificação, em cumprimento do contrato do PRR, e a certificação de organismos da Administração Pública neste Esquema.

No plano internacional , o DRSC continuará a contribuir para o desenvolvimento dos esquemas europeus de certificação da cibersegurança EU Cloud Services e EU5G, e a participar em processos de regulação da certificação europeia.

O DRSC procurará promover a divulgação e a adoção dos esquemas nacionais EC QNRCS e EC Empresas de serviços de cibersegurança, e do esquema europeu EU Common Criteria, através de iniciativas de informação, sensibilização e divulgação junto de interessados, como candidatos ou organismos de avaliação da conformidade.

CISO GNS / CNCS

Para cumprimento das funções de CISO em 2024, será elaborado e entregue o Relatório Anual referente a 2023, previsto no Regime Jurídico da Segurança do Ciberespaço. Será finalizada a Política de Utilização de Equipamento corporativo e serão realizadas duas avaliações de maturidade de cibersegurança. Procurar-se-á continuar a desenvolver uma política de gestão de incidentes e dar início à elaboração de um plano de Segurança GNS/CNCS.

Conselho Superior de Segurança do Ciberespaço

O DRSC assegura e gere as atividades do Conselho Superior de Segurança do Ciberespaço e da Comissão de Avaliação de Segurança, criada na sua dependência, prevendo-se a continuação de um elevado grau de dedicação da equipa DRSC às atividades deste foro, como a gestão de reuniões.

Outros projetos e atividades

Cibersegurança das eleições

Em função da ocorrência de três exercícios eleitorais em Portugal em 2024 e do conhecimento e experiência adquiridos no WS do Cooperation Group sobre as eleições, existe um forte envolvimento do DRSC nesta atividade. Irá, assim, contribuir em grande medida para a realização de exercício nacional focado na cibersegurança de eleições, em 9 de fevereiro, e para a redação de atualização de compendium de cibersegurança das eleições no âmbito do WS citado.

Comissão de Planeamento de Emergência da Cibersegurança

Ativada a Comissão de Planeamento de Emergência da Cibersegurança, criada no contexto do Sistema Nacional de Planeamento Civil de Emergência, instituído pelo Decreto-Lei n.º 43/2020, de 21 de julho, e gerida pelo DRSC, o corrente ano será dedicado à Identificação de entidades e infraestruturas digitais críticas.

OBJETIVOS OPERACIONAIS

DRSC_PI113 – Definir os processos de supervisão e especificar requisitos para ferramenta de suporte.

Indicador: Entrega do estudo sobre os processos de supervisão da cibersegurança.

Meta: 30 de abril.

DRSC_PI114 – **OP1** Finalizar o projeto de regulamento relativo à implementação do RJSC na Administração Pública **(Objetivo operacional do QUAR 2024).**

Indicador: Enviar para a Tutela de projeto de Regulamento juríco do Ciberespaço (RJSC).

Meta: 31 de maio.

DRSC_P122 – Promover o estabelecimento de entidades certificadoras no EC QNRCS.

Indicador: Número de entidades certificadoras acreditadas pelo IPAC.

Meta: 2.

DEPARTAMENTO DE SERVIÇOS TÉCNICOS (DST)

O Departamento 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.

Gestão de Sistemas e Infraestruturas (GSI)

A área de Gestão de Sistemas e Infraestruturas assegura a disponibilização, gestão e manutenção dos sistemas de suporte ao CERT.PT e à Rede Corporativa do GNS/CNCS. No seu âmbito, são também desenvolvidas atividades regulares de apoio à manutenção da Infraestrutura, de onde se destaca a renovação do parque de servidores, a atualização da infraestrutura de virtualização e diversas operações de manutenção e atualização de software.
Nesse sentido, em 2024 será dada prioridade à migração do parque informático Linux assente em CentOS 7, cujo suporte termina a 30 junho de 2024, para Rocky Linux 9.

Apoio ao utilizador (AU)

No que diz respeito à área de Apoio ao Utilizador, e para além das tarefas recorrentes de intervenção ao nível dos postos de trabalho, será mantida a aposta na renovação dos equipamentos afetos aos utilizadores, sempre que tal se justifique.

Na sequência da necessidade de adaptação a um modelo de trabalho híbrido, e de forma a facilitar a comunicação externa e interna no âmbito da transição entre trabalho remoto e presencial, serão implementadas novas formas de reunir, com recurso a cabines de escritório acústicas, que permitirão a realização de reuniões sem prejuízo dos restantes colegas de sala.

O apoio ao utilizador precisa de ser sistematizado e organizado para uma melhor resposta e um melhor acompanhamento do desenrolar das tarefas por parte dos interessados. Assim sendo, em 2024, irá ser implementado um portal de pedidos que englobará pedidos de serviço, reporte de problemas e marcação de salas e cabines, será implementado um serviço de resposta interativa por telefone (IVR), que permitirá uma melhor resposta às solicitações telefónicas.

Adicionalmente é necessária a renovação da capacidade audiovisual da sala de reuniões do Centro, que é limitada aquando da realização de reuniões em formato híbrido.

Security Operations Center (SOC)

No âmbito da sua atividade regular, o Secuity Operations Center (SOC) do CNCS manterá a aposta num conjunto alargado de atividades operacionais, nomeadamente a operação do SIEM e consolidação de fontes de dados; a análise de eventos de segurança; a publicação de relatórios semanais com os principais eventos de segurança registados; o envio de alertas de segurança relevantes a toda a comunidade servida; a ligação com o CISO; e a execução da política de gestão de vulnerabilidades e de patches.

Dando continuidade ao trabalho iniciado em 2023 com o desenho do Plano de Continuidade de Negócio, iremos em 2024, iniciar a implementação do mesmo.

OBJETIVOS OPERACIONAIS

DST_P123 – **OP4** Migrar os sistemas prioritários baseados em Linux para versões atualizadas do sistema operativo **(Objetivo operacional do QUAR 2024).**

Indicador: Data de entrada dos serviços em produção.

Meta: 30 de junho.

DST_G209 – Implementar os objetivos de médio prazo do Plano de Continuidade de Negócio.

Indicador: Entrada em produção dos serviços atualizados.

Meta: 31 de dezembro.

DST_P129 – Implementar o portal de pedidos.

Indicador: Serviços em produção do portal.

Meta: 31 de dezembro.

RECURSOS HUMANOS

A estrutura de recursos humanos do GNS e do CNCS compreende pessoal das Forças Armadas (FA), Forças de Segurança (FS-GNR/PSP), disponibilizado e remunerado pelos serviços de origem (FA e FS), e pessoal civil, proveniente quer do setor público quer do setor privado.

Em 01 de janeiro de 2023 o GNS dispunha de 122 postos de trabalho previstos no mapa de pessoal, tendo conseguido ainda durante o mesmo ano um incremento de 33 novos postos de trabalho dos quais 31 a afetar ao CNCS e 2 ao GNS, aprovado por Despacho Interno n.º 110/2023/MF do Ministro das Finanças, exarado sobre o Despacho n.º 368/2023/SEO da Secretária de estado do Orçamento, para o ano de 2023, de 33 novos postos de trabalho, 31 dos quais a afetar ao CNCS, tendo sido autorizado o reforço orçamental de despesas com pessoal por Despacho n.º 730/2023/SEO, de 31 de agosto, da Secretária de Estado do Orçamento.

Em 2024 irá prosseguir-se o esforço de recrutamento de pessoal, afigurando-se como necessário, para que o GNS/CNCS assegure as suas atribuições, o preenchimento de 156 postos de trabalho.

O quadro seguinte projeta, de acordo com o Mapa de Pessoal aprovado para 2024 (ANEXO E), os quantitativos globais de pessoal necessário para o desempenho das atribuições do GNS e do CNCS.

RESUMO – RECURSOS HUMANOS

Proveniência/natureza	Quantitativos	
	GNS	CNCS
Forças Armadas (militares)	62	0
Forças de Segurança (GNR/PSP)	13	0
Civis	10	71
Sub Totais	**85**	**71**
TOTAL	**156**	

Categoria/Qualificação	Quantitativos	
	GNS	CNCS
Dirigentes Superiores	1 Diretor Geral	
	1 Subdiretor Geral	1 subdiretor Geral
Oficiais das Forças Armadas	27	-
Sargentos das Forças Armadas	32	-
Praças das Forças Armadas	10	-
Agentes da PSP	3	-
Técnicos Superiores	2	-
Consultores Coordenadores	-	5
Consultores	4	10
Técnicos		54
Assistentes Técnicos	3	1
Assistentes Operacionais	2	-
Sub Totais	**85**	**71**
TOTAL	**156**	

RECURSOS FINANCEIROS

O Orçamento do Estado 2024, conforme o seguinte quadro, foi planeado de Receitas de Impostos (Fonte de Financiamento (FF) 311) para o GNS (Atividade 231) o montante de 781.049,00€ e para o CNCS (Atividade

171) o montante de 4.049.951,00€, e em Receitas Próprias (FF 531) foi planeado para o GNS (Atividade 231) o montante de 1.580.900,00€, totalizando 6.411.900,00€.

Funcionamento	FF 311 Atividade 231 GNS	Agrupamento 01 - Pessoal	603.933,00 €
		Agrupamento 02 - Bens e Serviços	177.116,00 €
		Agrupamento 07 - Despesas Capital	0,00€
		Subtotal 231	*781.049,00€*
	FF 311 Atividade 171 CNCS	Agrupamento 01 - Pessoal	3.383.217,00 €
		Agrupamento 02 - Bens e Serviços	510.875,00 €
		Agrupamento 07 - Despesas Capital	155.859,00 €
		Subtotal 171	*4.049.951,00 €*
		Total FF 311	4.831.000,00 €
	FF 513 Atividade 231 GNS	Agrupamento 01 - Pessoal	25.000,00 €
		Agrupamento 02 - Bens e Serviços	945.900,00 €
		Agrupamento 06 - Reserva	39.523,00 €
		Agrupamento 07 - Despesas Capital	570.477,00 €
		Total FF 513	1.580.900,00 €
		Total FF 311 + FF513	6.411.900,00 €

Para 2024, foram planeados os projetos que constam no Anexo E e respetivos montantes por classificação económica de despesa (CED), com financiamentos de Fundos Europeus e (FF 482) e PRR (FF483 e 484).

PLANO DE FORMAÇÃO

A formação é um instrumento de promoção do desenvolvimento organizacional através da otimização do potencial individual e coletivo disponível na organização. Visa a capacitação para um desempenho superior na realização das atividades que concretizam a estratégia delineada.

Considerando o total de postos de trabalho, as diferentes áreas de atividade do GNS e do CNCS e a evolução prevista das necessidades de pessoal, vertidas no respetivo Mapa, foi realizado o levantamento dos requisitos de formação, tendo por base a consulta aos chefes de unidades orgânicas e pontualmente aos trabalhadores.

O Plano de Formação resultante prevê as ações adequadas para a aquisição e desenvolvimento de conhecimentos e competências que conduzam ao incremento do desempenho profissional, bem como à valorização pessoal e profissional dos trabalhadores.

O montante previsto despender com a formação dos recursos humanos do GNS/CNCS é, aproximadamente, de 739.370,00€, sendo cerca de 676.550,00 resultante do PRR, sendo o restante valor, cerca de 62.820€, suportado pelo orçamento de estado 2024.

MEDIDAS DE MODERNIZAÇÃO ADMINISTRATIVA

Em cumprimento do disposto no Decreto-Lei n.º 135/99, de 22 de abril, referente a medidas de modernização administrativa, o GNS/CNCS propõe-se prosseguir com a atenuação da carga burocrática dos processos, desmaterialização de documentos administrativos e simultaneamente ajustar o conteúdo do seu portal web no sentido de facilitar e simplificar a interação, no acesso e requisição dos serviços pelos utentes, contribuindo assim para uma administração pública mais ágil, amiga e próxima do utilizador.

Assim, em 2024, o GNS/CNCS propõe-se prosseguir com a consolidação do alcançado anteriormente, efetuando melhorias e implementado novas funcionalidades, que se revelem necessárias ao funcionamento do sistema de Credenciações de Segurança Online (CRESO), a fim de facilitar a requisição de serviços pelos utentes, e dar continuidade às seguintes atividades:

- Prosseguir com a implementação das novas funcionalidades e melhorias (eSEIF 2.0 e eSEIF Light) do Sistema de Gestão da Informação Classificada (SEIF)

- Prosseguir a transformação digital, designadamente através da evolução do sistema de gestão documental que está em produção, que potenciará a capacitação para a gestão da informação como potenciador da estratégia (reforçar as soluções colaborativas internas, prosseguir a implementação das políticas de modernização administrativa e desenvolver soluções de apoio à decisão, em alinhamento com a estratégia e Programa do XXIII Governo) e ainda modernizando profundamente os processos e tecnologia associados à gestão e controlo interno.

No âmbito da implementação do Regime Geral de Prevenção da Corrupção (RGPC), o GNS/CNCS propõe-se a assegurar a plena implementação do Plano de Prevenção de Risco de Corrupção e Infrações Conexas (PPRCIC), garantindo o correto funcionamento do Canal de Denúncias e da implementação de um plano de formação e comunicação adequado às suas necessidades.

PUBLICIDADE INSTITUCIONAL

A Lei n.º 95/2015, de 17 de agosto, no n.º 2 do art.º 7.º, define as regras e os deveres de transparência quanto à realização de campanhas de publicidade institucional do Estado. O GNS não prevê a realização de qualquer campanha de publicidade institucional ou a aquisição de espaço publicitário no corrente ano.

No âmbito da *C-Academy* o CNCS pretende, no garante das regras estabelecidas, efetuar a divulgação deste Programa Nacional com recurso a vários meios de comunicação (Televisão, rádio e principais redes sociais).

Lisboa, 05 de abril de 2024

O DIRETOR-GERAL

António José Gameiro Marques
CALM

Anexos:

Anexo A – Plano de Formação do GNS
Anexo B – Plano de Formação do CNCS
Anexo C - QUAR
Anexo D – Proposta de Orçamento
Anexo E – Mapa de Pessoal
Anexo F – Código de Ética e Conduta
Anexo G – Plano de Prevenção de Riscos e Corrupção e Infrações Conexas

PÁGINA DEIXADA EM BRANCO

ANEXOS

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

ANEXO A – PLANO DE FORMAÇÃO DO GNS

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

Aprovo.

O Diretor Geral

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2024.03.15 09:38:50 Z

António Gameiro Marques
CALM

ANEXO A
Plano de Formação para 2024
GNS

Tabela A.1 - FORMAÇÃO FINANCIADA PELAS RECEITAS PRÓPRIAS DO GNS (FF513)

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
GNS/RP/PF2024/01	DC (ASSJUR + SDTI)	NATO Security Course		Oberammergau	EU	TBD	35	7	4	MIL - OFGEN / OFSUP	450,00 €	RP/ GNS	1 800,00 €	2 000,00 €	4 800,00 €	120,00 €	2 334,95 €	11 054,95 €	1	A única vaga que está garantida é a do COR Mota Pereira, porque foi cancelada em 2023 por causa dos problemnas com o mau tempo nos aeroportos. As restantes vagas foram inscritas em lista de espera para eventuais desistências.
GNS/RP/PF2024/02	NAD (ASSJUR)	E-Curso Proteção de Dados Pessoais		NOVA School of Law	PT-LX	TBD	17	5	1	MIL - OFGEN / OFSUP	450,00 €	RP/ GNS	450,00 €	0,00 €	0,00 €	0,00 €	0,00 €	450,00 €	1	
GNS/RP/PF2024/03	NAD (ASSJUR)	Pós-graduação em Comunicação e Psicologia Positiva: Contributos para o Bem Estar das Organizações		Universidade Católica	PT-LX	01/10/2024	130		1	CIV - SUP NIVEL 18	3 165,00 €	RP/ GNS	3 165,00 €	0,00 €	0,00 €	0,00 €	0,00 €	3 165,00 €	1	
GNS/RP/PF2024/04	DIA	Avaliação e Gestão de Sistemas de Security		APSEI	PT-LX	TBD	12	2	2	MIL - OFSUB / SMOR / SCH	209,10 €	RP/ GNS	418,20 €	0,00 €	0,00 €	0,00 €	0,00 €	418,20 €	1	
GNS/RP/PF2024/05	DIA	O Papel da Auditoria Interna na Prevenção dos Riscos de Corrupção		IPAI	PT-LX	TBD	8	2	1	MIL - OFGEN / OFSUP	307,50 €	RP/ GNS	307,50 €	0,00 €	0,00 €	0,00 €	0,00 €	307,50 €	1	
GNS/RP/PF2024/06	DIA	Como Realizar uma Auditoria Interna		IPAI	PT-LX	TBD	8	2	1	MIL - OFGEN / OFSUP	307,50 €	RP/ GNS	307,50 €	0,00 €	0,00 €	0,00 €	0,00 €	307,50 €	1	
GNS/RP/PF2024/07	DIA	Ética em Auditoria Interna		IPAI	PT-LX	02/12/2024	2	1	1	MIL - OFGEN / OFSUP	92,95 €	RP/ GNS	92,95 €	0,00 €	0,00 €	0,00 €	0,00 €	92,95 €	1	
GNS/RP/PF2024/08	DIA	APCER - Curso - A ISO 9001:2015 e a Gestão do Risco		APCER	PT-LX	19/03/2024	16	2	2	CIV - NIVEIS 9 A 18	456,00 €	RP/ GNS	912,00 €	0,00 €	0,00 €	0,00 €	0,00 €	912,00 €	1	O valor dos custos terá uma redução de 5%, por haver 2 inscrições da mesma organização; O valor total para estas formações, será de 912,00€ (novecentos e doze euros) [480,00 x 2 = 960,00 € >> Desconto de 5% = 48 € >> Total: 912,00 €]
GNS/RP/PF2024/09	DGICC - AND	ACO Courrier Service Training		SHAPE, Mons	EU	TBD	30	6	3	MIL - OFSUB / SMOR / SCH	0,00 €	RP/ GNS	0,00 €	1 500,00 €	3 000,00 €	75,00 €	1 408,81 €	5 983,81 €	1	
GNS/RP/PF2024/10	DGICC - AND	EU COMSEC Training Seminar		GSC, Bruxelas	EU	TBD	20	4	2	MIL - OFSUB / SMOR / SCH	0,00 €	RP/ GNS	0,00 €	1 000,00 €	1 200,00 €	30,00 €	626,14 €	2 856,14 €	1	
GNS/RP/PF2024/11	SDTI - ST	BlockChain Foundation		Online	PT-LX	(TBC)	18	3	1	MIL - OFGEN / OFSUP	250,00 €	RP/ GNS	250,00 €	0,00 €	0,00 €	0,00 €	0,00 €	250,00 €	1	
GNS/RP/PF2024/12	SDTI - ST	Professional Blockchain Business		PT-Lisboa	PT-LX	(TBC)	12	2	1	MIL - OFGEN / OFSUP	850,00 €	RP/ GNS	850,00 €	0,00 €	0,00 €	0,00 €	0,00 €	850,00 €	2	
GNS/RP/PF2024/13	SDTI - ST	EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION ACADEMY/ EITC/QI/QIF Quantum Information Fundamentals		Online	PT-LX	(TBC)	15	0	2	MIL - OFGEN / OFSUP	220,00 €	RP/ GNS	440,00 €	0,00 €	0,00 €	0,00 €	0,00 €	440,00 €	1	
GNS/RP/PF2024/14	SDTI - ST	EUROPEAN INFORMATION TECHNOLOGIES CERTIFICATION ACADEMY/ EITC/IS/QCF Quantum Cryptography Fundamentals		Online	PT-LX	(TBC)	15	0	2	MIL - OFGEN / OFSUP	220,00 €	RP/ GNS	440,00 €	0,00 €	0,00 €	0,00 €	0,00 €	440,00 €	1	
GNS/RP/PF2024/15	SDTI - SI	Sistemas de videovigilanacia - Avançado		On-line/Lx	PT-LX	TBD	24	0	2	MIL - OFGEN / OFSUP	1 228,00 €	RP/ GNS	2 456,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 456,00 €	1	
GNS/RP/PF2024/16	SDTI - SI	Curso de Defesa Nacional 2024/2025		IDN - Lisboa	PT-LX	04/11/2024	210	70	1	MIL - OFSUB / SMOR / SCH	500,00 €	RP/ GNS	500,00 €	0,00 €	0,00 €	0,00 €	0,00 €	500,00 €	1	Validado pelo art^{o}3º e 14º do regulamento. Mais-valia para o conhecimento atual das capacidades da Segurança e Defesa Nacional.
GNS/RP/PF2024/17	DSTI - SI	Redes Informaticas Aplicadas aos Sistemas Electronicos de Segurança		On-line/Lx	PT-LX	TBD	7	1	1	MIL - OFGEN / OFSUP	260,00 €	RP/ GNS	260,00 €	0,00 €	0,00 €	0,00 €	0,00 €	260,00 €	2	
GNS/RP/PF2024/18	DC	STARING YOUR ENGLISH JOURNEY/NIVEL INICIAL		INA	PT-LX	TBD	25	0	4	MIL - OFSUB / SMOR / SCH	250,00 €	RP/ GNS	1 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 000,00 €	1	
GNS/RP/PF2024/19	DC	ENGLISH FOR THE OFFICE/NIVEL INTERMÉDIO		INA	PT-LX	TBD	25	0	4	MIL - OFSUB / SMOR / SCH	250,00 €	RP/ GNS	1 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 000,00 €	1	

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
GNS/RP/PF2024/20	DC	INSTRUMENTOS NORMATIVOS DE PROTEÇÃO DE DADOS		INA	PT-LX	TBD	14	0	2	MIL - OFSUB / SMOR / SCH	140,00 €	RP/ GNS	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
GNS/RP/PF2024/21	DC	ATENDIMENTO AO CIDADÃO		INA	PT-LX	TBD	14	0	2	MIL - OFSUB / SMOR / SCH	140,00 €	RP/ GNS	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
GNS/RP/PF2024/22	DC	Adobe Acrobat Professional		INA	Online	TBD		0	4	CIV - INF NIVEL 9	0,00 €	RP/ GNS	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	Curso gratuito.
GNS/RP/PF2024/23	IRC	Administração e Configuração de Windows Server 2022		Rumos, LX	PT-LX	TBD	35	5	1	MIL - OFGEN / OFSUP	1 722,00 €	RP/GNS	1 722,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 722,00 €	2	
GNS/RP/PF2024/24	IRC	DevOps Engineering Foundation (DOEF)		Rumos, LX	PT-LX	TBD	16	3	1	MIL - OFGEN / OFSUP	1 131,60 €	RP/GNS	1 131,60 €	0,00 €	0,00 €	0,00 €	0,00 €	1 131,60 €	2	
GNS/RP/PF2024/25	IRC	Mestrado Cibersegurança e Informatica Forense		Leiria	PT-CONT	ano lectivo 2023-24			1	MIL - SAJ / 1SAR / 2SAR	1 140,00 €	RP/GNS	1 140,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 140,00 €	1	Propinas do 2º ano do Mestrado Instituto Politécnico de Leiria
GNS/RP/PF2024/26	IRC	Certified SOC Analyst (CSA)		Rumos, LX	PT-LX	TBD	24	3	1	MIL - SAJ / 1SAR / 2SAR	2 583,00 €	RP/GNS	2 583,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 583,00 €	2	
GNS/RP/PF2024/27	IRC	VMware vSphere: Install, Configure, Manage [v8]		Rumos, LX	PT-LX	TBD	40	5	1	MIL - SAJ / 1SAR / 2SAR	3 628,50 €	RP/GNS	3 628,50 €	0,00 €	0,00 €	0,00 €	0,00 €	3 628,50 €	2	
GNS/RP/PF2024/28	IRC	Hardening de Sistemas		Rumos, LX	PT-LX	TBD	21	8	1	MIL - PRAÇA	1 420,65 €	RP/GNS	1 420,65 €	0,00 €	0,00 €	0,00 €	0,00 €	1 420,65 €	2	
GNS/RP/PF2024/29	IRC	DevOps with Docker & Kubernetes		Rumos, LX	PT-LX	TBD	28	5	1	MIL - OFSUB / SMOR / SCH	1 400,00 €	RP/GNS	1 400,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 400,00 €	2	
GNS/RP/PF2024/30	IRC	Máquinas de Cifra - TCE		EMGFA - Lisboa	PT-LX	TBD	1	2	4	MIL - OFGEN / OFSUP	0,00 €	RP/GNS	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
GNS/RP/PF2024/31	ADMLOG	Pós-graduação em Contabilidade e Gestão Financeira na AP		INA	PT-LX	11/03/2024	150		1	CIV - NIVEIS 9 A 18	1 500,00 €	RP/GNS	1 500,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 500,00 €	1	O valor da propina é de 1.500,00 euros, com bolsa PRR de 750,00 euros. O valor relativo à propina (1.500,00 euros) deverá ser pago na totalidade antes do inico da Pós-graduação, sendo devolvido o valor da bolsa após término da pós-graduação com emissão do respetivo certificado de conclusão.
GNS/RP/PF2024/32	OFSEG	Evacuação de Edifícios		On-line/Lx	PT-LX	TBD	7	1	1	MIL - OFGEN / OFSUP	142,68 €	RP/GNS	142,68 €	0,00 €	0,00 €	0,00 €	0,00 €	142,68 €	1	
GNS/RP/PF2024/33	OFSEG	Gestão da Emergência: Do Planeamento à Avaliação de Exercícios		APSEI - Sacavém	PT-LX	TBD	14	2	1	MIL - OFSUB / SMOR / SCH	356,70 €	RP/GNS	356,70 €	0,00 €	0,00 €	0,00 €	0,00 €	356,70 €	1	
GNS/RP/PF2024/34	OFSEG	Sensibilização em Primeiros Socorros		GNS	PT-LX	TBD	7	1	1	MIL - OFGEN / OFSUP	660,00 €	RP/GNS	660,00 €	0,00 €	0,00 €	0,00 €	0,00 €	660,00 €	1	
GNS/RP/PF2024/35	OFSEG	Sensibilização em Combate a Incêndios e Evacuação de Edifícios (7 horas)		ENB - Sintra	PT-LX	TBD	7	1	1	MIL - OFGEN / OFSUP	1 270,00 €	RP/GNS	1 270,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 270,00 €	1	
													32 164,28 €	**4 500,00 €**	**9 000,00 €**	**225,00 €**	**4 369,89 €**	**50 259,17 €**		
															Transp. + Estadas	**13 725,00 €**				

ANEXO A.1
Plano de Formação para 2024
GNS

Tabela A.2 - FORMAÇÃO FINANCIADA PELO PRR (Submedida TD C19.i03.1.4 + Medida TD C19.i03.2 + Medida TD C19.i03.4 // FF483)

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS						Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL	
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo		
GNS/PRR/PF2024/01	NAD (PMO)	Business Intelligence; Analytics and Analysis		Smarter Execution	Online	02/05/2024	27	7	2	MIL - OFGEN / OFSUP	700,00 €	PRR Medida 1	1 400,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 400,00 €	1	Medida TD C19.i03.1 / Submedida TD C19.i03.1.4 / Meta 1362
GNS/PRR/PF2024/02	NAD (PMO + ASSJUR)	Iniciação à gestão de projetos		INA	PT-LX	TBD	21	3	2	MIL - OFGEN / OFSUP	210,00 €	PRR Medida 4	420,00 €	0,00 €	0,00 €	0,00 €	0,00 €	420,00 €	1	Medida TD C19.i03.4 / Submedida TD C19.i03.4.1 / Meta 1380
GNS/PRR/PF2024/03	NAD (PMO + ASSJUR)	Gestão de projetos no âmbito do PRR | Workshops		INA	PT-LX	TBD	91	17	3	MIL - OFGEN / OFSUP	875,00 €	PRR Medida 1	2 625,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 625,00 €	1	Medida TD C19.i03.1 / Submedida TD C19.i03.1.4 / Meta 1362
GNS/PRR/PF2024/04	NAD (PMO)	Preparação para a certificação seguindo os referenciais PM2 e ICB4		INA	PT-LX	TBD	91	17	2	MIL - OFGEN / OFSUP	280,00 €	PRR Medida 1	560,00 €	0,00 €	0,00 €	0,00 €	0,00 €	560,00 €	1	Medida TD C19.i03.1 / Submedida TD C19.i03.1.4 / Meta 1362
GNS/PRR/PF2024/05	NAD (OFSEG)	Gestão e Direção de Segurança		Autonoma Academy	PT-LX	TBD	251	0	1	MIL - OFGEN / OFSUP	1 750,00 €	PRR Medida 4	1 750,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 750,00 €	1	Medida TD C19.i03.4 / Submedida TD C19.i03.4.1 / Meta 1380
GNS/PRR/PF2024/06	IA + GICC + DC	Information Security 27001 Foundation		Behavior	PT-LX	TBD	16	3	5	MIL - OFGEN / OFSUP	420,00 €	PRR Medida 2	2 100,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 100,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.8 / Meta Interna (GAIA)
GNS/PRR/PF2024/07	IA	Risk Management 31000 Lead Manager		Behavior	PT-LX	TBD	40	4	1	MIL - OFGEN / OFSUP	2 050,00 €	PRR Medida2	2 050,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 050,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.8 / Meta Interna (GAIA)
GNS/PRR/PF2024/08	IA	Curso de Iniciação: Audit Risk Assessment Avaliação dos Riscos em Auditoria Interna		IPAI	PT-LX	TBD	32	8	1	MIL - OFGEN / OFSUP	861,00 €	PRR Medida2	861,00 €	0,00 €	0,00 €	0,00 €	0,00 €	861,00 €	2	Medida TD C19.i03.2 / Submedida TD C19.i03.2.8 / Meta Interna (GAIA)
GNS/PRR/PF2024/09	IA	Curso Intensivo de Auditoria Interna		IPAI	PT-LX	04/03/2024	32	8	1	MIL - OFGEN / OFSUP	861,00 €	PRR Medida2	861,00 €	0,00 €	0,00 €	0,00 €	0,00 €	861,00 €	2	Medida TD C19.i03.2 / Submedida TD C19.i03.2.8 / Meta Interna (GAIA)
GNS/PRR/PF2024/10	GICC - AND	DACAN Key Management Infrastructure (DKMI) Course		Maryland, EUA	Fora EU	05/02/2024	60	15	2	MIL - OFSUB / SMOR / SCH	0,00 €	PRR Medida2	0,00 €	2 400,00 €	5 600,00 €	140,00 €	2 348,01 €	10 488,01 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.4 / Meta 19.8
GNS/PRR/PF2024/11	GICC - AND	DACAN Key Management Infrastructure (DKMI) Course		Maryland, EUA	Fora EU	TBD	60	15	2	MIL - OFSUB / SMOR / SCH	0,00 €	PRR Medida2	0,00 €	2 400,00 €	5 600,00 €	140,00 €	2 348,01 €	10 488,01 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.4 / Meta 19.9
GNS/PRR/PF2024/12	GICC - AND	Crypto Administration (A0004)		NCI Academy	PT-LX	TBD	30	5	2	MIL - OFSUB / SMOR / SCH	1 160,00 €	PRR Medida2	2 320,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 320,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.4 / Meta 19.10
GNS/PRR/PF2024/13	GICC - AND	CARDS for NATO Crypto Custodian (A0006)		NCI Academy	PT-LX	TBD	30	5	2	MIL - OFSUB / SMOR / SCH	1 160,00 €	PRR Medida2	2 320,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 320,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.4 / Meta 19.11
GNS/PRR/PF2024/14	GICC - AND	TCE 621 Operator Course		Oslo, Norway	EU	TBD	30	5	2	MIL - OFGEN / OFSUP	0,00 €	PRR Medida2	0,00 €	1 000,00 €	1 600,00 €	40,00 €	833,91 €	3 473,91 €	1	O valor do curso está contratado no âmbito do procedimento n.º 03-AD-2024 - Aquisição e sustentação de equip Criptográficos TCE621 Medida TD C19.i03.2 / Submedida TD C19.i03.2.4 / Meta 19.12
GNS/PRR/PF2024/15	SDTI - ST	CISSP® - Certified Information Systems Security Professional - RUMOS		PT-Lisboa	PT-LX	13/05/2024	35	5	1	MIL - OFGEN / OFSUP	3 400,00 €	PRR	3 400,00 €	0,00 €	0,00 €	0,00 €	0,00 €	3 400,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.1 / Meta 1364
GNS/PRR/PF2024/16	SDTI - ST	Cloud Security Professional		On-line/Lx	PT-LX	(TBC)	35	5	1	MIL - OFGEN / OFSUP	2 250,00 €	RP/GNS	2 250,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 250,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.1 / Meta 1364
GNS/PRR/PF2024/17	SDTI - SE	Galileu Security Monitor Center - GRON Operators		Paris	EU	05/02/2024	32	5	2	MIL - OFGEN / OFSUP	0,00 €	PRR Medida2	0,00 €	1 000,00 €	1 600,00 €	40,00 €	833,91 €	3 473,91 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.7 / Meta Interna (Seg Esp.)
GNS/PRR/PF2024/18	SDTI - SE	Galileu Security Monitor Center - GRON Technician		Paris	EU	12/02/2024	24	4	1	MIL - OFGEN / OFSUP	0,00 €	PRR Medida2	0,00 €	500,00 €	600,00 €	15,00 €	333,56 €	1 448,56 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.7 / Meta Interna (Seg Esp.)
GNS/PRR/PF2024/19	SDTI - SE	EUSPA - EU Crypto training		Praga	EU	12/03/2024	16	3	1	MIL - OFGEN / OFSUP	0,00 €	PRR Medida2	0,00 €	500,00 €	400,00 €	10,00 €	250,17 €	1 160,17 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.7 / Meta Interna (Seg Esp.)

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS						Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL	
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo		
GNS/PRR/PF2024/20	SDTI - SC	Curso eIDAS Professional		Essen (Alemanha)	EU	13/05/2024	40	6	2	MIL - OFGEN / OFSUP	3 500,00 €	PRR Medida2	7 000,00 €	1 000,00 €	2 000,00 €	50,00 €	1 000,69 €	11 050,69 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.5 / Meta 1368
GNS/PRR/PF2024/21	SDTI - SC	ISO 27001 Lead Auditor		On Line	PT-LX	(TBC)	40	5	1	MIL - OFGEN / OFSUP	2 350,00 €	RP/GNS	2 350,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 350,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.5 / Meta 1368
GNS/PRR/PF2024/22	SDTI - SC	Information Security Manager (CISM preparation course)		On Line	PT-LX	(TBC)	24	3	2	MIL - OFGEN / OFSUP	1 600,00 €	RP/GNS	3 200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	3 200,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.5 / Meta 1368
GNS/PRR/PF2024/23	DC	Interpretação ISO/IEC 27001:2022- Sistemas de Gestão de Segurança de Informação		Behavior	PT-LX	TBD	16	2	3	MIL - OFGEN / OFSUP	480,00 €	PRR Medida2	1 440,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 440,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.6 / Meta 1369
GNS/PRR/PF2024/24	DC	Boas Práticas de auditorias ISO 19011:2018– Case study ISO/IEC 27001:2022		Behavior	PT-LX	TBD	40	3	1	MIL - OFGEN / OFSUP	720,00 €	PRR Medida2	720,00 €	0,00 €	0,00 €	0,00 €	0,00 €	720,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.6 / Meta 1369
GNS/PRR/PF2024/25	IRC	Implementing and Operating Cisco Collaboration Core Technologies (CLCOR)		Rumos, LX	PT-LX	TBD	35	5	1	MIL - OFGEN / OFSUP	4 243,50 €	PRR Medida2	4 243,50 €	0,00 €	0,00 €	0,00 €	0,00 €	4 243,50 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/26	IRC	Fundamentos de Windows Server 2022		Rumos, LX	PT-LX	TBD	35	5	1	MIL - OFGEN / OFSUP	1 506,75 €	PRR Medida2	1 506,75 €	0,00 €	0,00 €	0,00 €	0,00 €	1 506,75 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/27	IRC	ISTQB® Certified Tester Foundation Level		Rumos, LX	PT-LX	TBD	21	3	1	MIL - OFGEN / OFSUP	1 537,50 €	PRR Medida2	1 537,50 €	0,00 €	0,00 €	0,00 €	0,00 €	1 537,50 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/28	IRC	Mestrado Informática		Lisboa	PT-LX	30/10/2024			1	MIL - OFSUB / SMOR / SCH	2 970,00 €	PRR Medida2	2 970,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 970,00 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/29	IRC	CompTIA Cybersecurity Analyst + CertPrep (CySA+)		Rumos, LX	PT-LX	TBD	35	5	1	MIL - SAJ / 1SAR / 2SAR	2 779,80 €	PRR Medida2	2 779,80 €	0,00 €	0,00 €	0,00 €	0,00 €	2 779,80 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/30	IRC	Check Point Administrator and Troubleshooting R81.20 (CCSA+CCTA)		Rumos, LX	PT-LX	TBD	35	5	1	MIL - SAJ / 1SAR / 2SAR	3 394,80 €	PRR Medida2	3 394,80 €	0,00 €	0,00 €	0,00 €	0,00 €	3 394,80 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/31	IRC	VMware vSphere: What's New [V6.7 to V7]		Rumos, LX	PT-LX	TBD	24	1	1	MIL - SAJ / 1SAR / 2SAR	2 287,80 €	PRR Medida2	2 287,80 €	0,00 €	0,00 €	0,00 €	0,00 €	2 287,80 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/32	IRC	Administering Microsoft Endpoint Configuration Manager		Rumos, LX	PT-LX	19/02/2024	35	5	1	MIL - OFSUB / SMOR / SCH	2 386,20 €	PRR Medida2	2 386,20 €	0,00 €	0,00 €	0,00 €	0,00 €	2 386,20 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/33	IRC	AZ-801: Configuring Windows Server Hybrid Advanced Services		Rumos, LX	PT-LX	TBD	28	4	1	MIL - PRAÇA	1 857,30 €	RP/GNS	1 857,30 €	0,00 €	0,00 €	0,00 €	0,00 €	1 857,30 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
GNS/PRR/PF2024/34	IRC	Red Hat Linux Diagnostics and Troubleshooting (RH342)		Rumos, LX	PT-LX	TBD	27	4	1	MIL - OFSUB / SMOR / SCH	3 124,20 €	PRR Medida2	3 124,20 €	0,00 €	0,00 €	0,00 €	0,00 €	3 124,20 €	1	Medida TD C19.i03.2 / Submedida TD C19.i03.2.2 / Meta 1365
													63 714,85 €	**8 800,00 €**	**17 400,00 €**	**435,00 €**	**7 948,27 €**	**98 298,12 €**		
															Transporte + Alojamento	**26 635,00 €**				

ANEXO B – PLANO DE FORMAÇÃO DO CNCS

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

PÁGINA DEIXADA EM BRANCO

ANEXO B
Plano de Formação para 2024
CNCS

Aprovo.

O Diretror Geral
António José Gameiro Marques
Digitally signed by António José Gameiro Marques
Date: 2024.03.15 09:38:14 Z
António Gameiro Marques
CALM

Tabela B.1 - FORMAÇÃO FINANCIADA PEL0 ORÇAMENTO DE FUNCIONAMENTO DO CNCS (FF311)

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
CNCS/OE/PF2024/01	DRSC	Direito para não juristas			Online	01/06/2024	14	2	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/02	DRSC	Direito para não juristas			Online	01/06/2024	14	2	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/03	DRSC	Código do Procedimento Administrativo para não juristas			Online	01/06/2024	18	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	
CNCS/OE/PF2024/04	DRSC	Código do Procedimento Administrativo para não juristas			Online	01/06/2024	18	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	
CNCS/OE/PF2024/05	DRSC	Código do Procedimento Administrativo para juristas			Online	01/06/2024	21	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	
CNCS/OE/PF2024/06	DRSC	Contencioso Administrativo			Online	01/06/2024	28	4	1	CIV - SUP NIVEL 18	280,00 €	OE	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
CNCS/OE/PF2024/07	DRSC	Contencioso Administrativo			Online	01/06/2024	28	4	1	CIV - SUP NIVEL 18	280,00 €	OE	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
CNCS/OE/PF2024/08	DRSC	Regime Geral das Contraordenações			Online	01/06/2024	28	4	1	CIV - SUP NIVEL 18	280,00 €	OE	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
CNCS/OE/PF2024/09	DRSC	Regime Geral das Contraordenações			Online	01/06/2024	28	4	1	CIV - SUP NIVEL 18	280,00 €	OE	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
CNCS/OE/PF2024/10	DRSC	Regime Geral das Contraordenações			Online	01/06/2024	28	4	1	CIV - SUP NIVEL 18	280,00 €	OE	280,00 €	0,00 €	0,00 €	0,00 €	0,00 €	280,00 €	1	
CNCS/OE/PF2024/11	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/12	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/13	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/14	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/15	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/16	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/17	DRSC	Introdução às Tecnologias Emergentes			Online	01/06/2024	6	1	1	CIV - SUP NIVEL 18	0,00 €	OE	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	
CNCS/OE/PF2024/18	DRSC	Legística formal aplicada			Online	01/06/2024	10	1	1	CIV - SUP NIVEL 18	100,00 €	OE	100,00 €	0,00 €	0,00 €	0,00 €	0,00 €	100,00 €	1	
CNCS/OE/PF2024/19	DRSC	Legística formal aplicada			Online	01/06/2024	10	1	1	CIV - SUP NIVEL 18	100,00 €	OE	100,00 €	0,00 €	0,00 €	0,00 €	0,00 €	100,00 €	1	
CNCS/OE/PF2024/20	DRSC	Legística formal aplicada			Online	01/06/2024	10	1	1	CIV - SUP NIVEL 18	100,00 €	OE	100,00 €	0,00 €	0,00 €	0,00 €	0,00 €	100,00 €	1	
CNCS/OE/PF2024/21	DRSC	Legística formal aplicada			Online	01/06/2024	10	1	1	CIV - SUP NIVEL 18	100,00 €	OE	100,00 €	0,00 €	0,00 €	0,00 €	0,00 €	100,00 €	1	
CNCS/OE/PF2024/22	DRSC	Preparação e redação de atos legislativos e de regulamentos			Online	01/06/2024	21	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
CNCS/OE/PF2024/23	DRSC	Preparação e redação de atos legislativos e de regulamentos			Online	01/06/2024	21	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	
CNCS/OE/PF2024/24	DRSC	Preparação e redação de atos legislativos e de regulamentos			Online	01/06/2024	21	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	
CNCS/OE/PF2024/25	DRSC	Preparação e redação de atos legislativos e de regulamentos			Online	01/06/2024	21	3	1	CIV - SUP NIVEL 18	210,00 €	OE	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	210,00 €	1	
CNCS/OE/PF2024/26	DRSC	ISO 27001 Implementer Foundation			Online	01/06/2024	16	2	1	CIV - SUP NIVEL 18	950,00 €	OE	950,00 €	0,00 €	0,00 €	0,00 €	0,00 €	950,00 €	1	
CNCS/OE/PF2024/27	DRSC	ISO 27001 Implementer Foundation			Online	01/06/2024	16	2	1	CIV - SUP NIVEL 18	950,00 €	OE	950,00 €	0,00 €	0,00 €	0,00 €	0,00 €	950,00 €	1	
CNCS/OE/PF2024/28	DRSC	ISO 27001 Implementer Foundation			Online	01/06/2024	16	2	1	CIV - SUP NIVEL 18	950,00 €	OE	950,00 €	0,00 €	0,00 €	0,00 €	0,00 €	950,00 €	1	
CNCS/OE/PF2024/29	DRSC	Gestão do risco			Online	01/06/2024	20	3	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/30	DRSC	Gestão do risco			Online	01/06/2024	20	3	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/31	DRSC	Gestão do risco			Online	01/06/2024	20	3	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/32	DRSC	Gestão do risco			Online	01/06/2024	20	3	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/33	DRSC	Gestão do risco			Online	01/06/2024	20	3	1	CIV - SUP NIVEL 18	200,00 €	OE	200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	200,00 €	1	
CNCS/OE/PF2024/34	DRSC	Fundamentos Básicos de Cibersegurança			PT-CONT	01/06/2024	35	5	1	CIV - SUP NIVEL 18	50,00 €	OE	50,00 €	80,00 €	300,00 €	0,00 €	250,10 €	680,10 €	1	
CNCS/OE/PF2024/35	DRSC	Princípios Técnicos em Cibersegurança			Online	01/06/2024	35	5	1	CIV - SUP NIVEL 18	50,00 €	OE	50,00 €	0,00 €	0,00 €	0,00 €	0,00 €	50,00 €	1	
CNCS/OE/PF2024/36	DRSC	Princípios Técnicos em Cibersegurança			Online	01/06/2024	35	5	1	CIV - SUP NIVEL 18	50,00 €	OE	50,00 €	0,00 €	0,00 €	0,00 €	0,00 €	50,00 €	1	
CNCS/OE/PF2024/37	DRSC	Princípios Técnicos em Cibersegurança			Online	01/06/2024	35	5	1	CIV - SUP NIVEL 18	50,00 €	OE	50,00 €	0,00 €	0,00 €	0,00 €	0,00 €	50,00 €	1	
CNCS/OE/PF2024/38	DRSC	Princípios Técnicos em Cibersegurança			Online	01/06/2024	35	5	1	CIV - SUP NIVEL 18	50,00 €	OE	50,00 €	0,00 €	0,00 €	0,00 €	0,00 €	50,00 €	1	
CNCS/OE/PF2024/39	DRSC	Princípios Técnicos em Cibersegurança			Online	01/06/2024	35	5	1	CIV - SUP NIVEL 18	50,00 €	OE	50,00 €	0,00 €	0,00 €	0,00 €	0,00 €	50,00 €	1	
													7 820,00 €	**80,00 €**	**300,00 €**	**0,00 €**	**250,10 €**	**7 630,10 €**		
															Transp. + Estadas	**380,00 €**				

ANEXO B
Plano de Formação para 2024
CNCS

Tabela B.2 - FORMAÇÃO FINANCIADA PELO PRR (Medida TD C19.i03.1 - Submedida TD C19.i03.1.4 + Medida TD C19.i03.3, FF483)

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
CNCS/PRR/PF2024/01	DST	Curso SANS a designar		Europa	EU	01/03/2024		5	1	CIV - SUP NIVEL 18	6 950,00 €	PRR C19	6 950,00 €	500,00 €	800,00 €	20,00 €	312,73 €	8 582,73 €	1	
CNCS/PRR/PF2024/02	DST	Curso SANS a designar		Europa	EU	01/03/2024		5	1	CIV - SUP NIVEL 18	6 950,00 €	PRR C19	6 950,00 €	500,00 €	800,00 €	20,00 €	312,73 €	8 582,73 €	1	
CNCS/PRR/PF2024/03	DST	Curso SANS a designar		Europa	EU	01/03/2024		5	1	CIV - SUP NIVEL 18	6 950,00 €	PRR C19	6 950,00 €	500,00 €	800,00 €	20,00 €	312,73 €	8 582,73 €	1	
CNCS/PRR/PF2024/04	DST	Curso SANS a designar		Europa	EU	01/03/2024		5	1	CIV - SUP NIVEL 18	6 950,00 €	PRR C19	6 950,00 €	500,00 €	800,00 €	20,00 €	312,73 €	8 582,73 €	1	
CNCS/PRR/PF2024/05	DST	Curso SANS a designar		Europa	EU	01/03/2024		5	1	CIV - SUP NIVEL 18	6 950,00 €	PRR C19	6 950,00 €	500,00 €	800,00 €	20,00 €	312,73 €	8 582,73 €	1	
CNCS/PRR/PF2024/06	DST	Formação a designar - Área de Sistemas		TBD	PT-CONT	01/03/2024		5	1	CIV - SUP NIVEL 18	2 500,00 €	PRR C19	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	
CNCS/PRR/PF2024/07	DST	Formação a designar - Área de Sistemas		TBD	PT-CONT	01/03/2024		5	1	CIV - SUP NIVEL 18	2 500,00 €	PRR C19	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	
CNCS/PRR/PF2024/08	DST	Formação a designar - Área de Redes/Segurança		TBD	PT-CONT	01/03/2024		5	1	CIV - SUP NIVEL 18	2 500,00 €	PRR C19	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	
CNCS/PRR/PF2024/09	DST	Formação a designar - SOC		TBD	PT-CONT	01/03/2024		5	1	CIV - SUP NIVEL 18	2 500,00 €	PRR C19	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	
CNCS/PRR/PF2024/10	DST	Formação a designar - Área de Sistemas		TBD	PT-CONT	01/03/2024		5	1	CIV - SUP NIVEL 18	2 500,00 €	PRR C19	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	
CNCS/PRR/PF2024/11	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/12	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/13	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/14	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/15	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/16	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	(incluída no Programa de formação Auditores ANCC + RJSC - ver lista de compras)
CNCS/PRR/PF2024/17	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	(incluída no Programa de formação Auditores ANCC + RJSC - ver lista de compras)
CNCS/PRR/PF2024/18	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/19	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
CNCS/PRR/PF2024/20	DO	SANS		Europa	EU	01/06/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/21	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/22	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/23	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/24	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/25	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/26	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/27	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/28	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/29	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/30	DO	SANS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	10 000,00 €	PRR C19	10 000,00 €	500,00 €	400,00 €	10,00 €	187,64 €	11 097,64 €	1	
CNCS/PRR/PF2024/31	DO	TRANSITS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/32	DO	TRANSITS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/33	DO	TRANSITS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/34	DO	TRANSITS		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/35	DO	TRANSITS II		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/36	DO	TRANSITS II		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/37	DO	TRANSITS II		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/38	DO	TRANSITS II		Europa	EU	01/09/2024		3	1	CIV - SUP NIVEL 18	1 500,00 €	PRR C19	1 500,00 €	500,00 €	400,00 €	10,00 €	187,64 €	2 597,64 €	1	
CNCS/PRR/PF2024/39	DCTO	SANS a designar		europa	EU	01/02/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/40	DCTO	SANS a designar		europa	EU	01/03/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	

ID	Un. Orgân.	Formação	Participantes	Local	Zona	Data de Inicio	Horas de formação	Dias da missão	Nº de Pessoas	Chefe da Equipa	Preço Unitário da Formação (Propinas + Inscrição)	ESTIMATIVA DE CUSTOS							Priorid. Unidade Orgânica	Observações
												FF	02.02.15.A/B	02.02.13			01.02.04	TOTAL		
													Formação	Transporte	Alojamento	Portagens e Tx. Cidade	Ajudas de custo			
CNCS/PRR/PF2024/41	DCTO	SANS a designar		online	Online	01/04/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	7 200,00 €	1	
CNCS/PRR/PF2024/42	DCTO	SANS a designar		online	Online	01/05/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	0,00 €	0,00 €	0,00 €	0,00 €	7 200,00 €	1	
CNCS/PRR/PF2024/43	DCTO	SANS a designar		europa	EU	01/06/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/44	DCTO	SANS a designar		europa	EU	01/07/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/45	DCTO	SANS a designar		europa	EU	01/08/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/46	DCTO	SANS a designar		europa	EU	01/09/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/47	DCTO	SANS a designar		europa	EU	01/10/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/48	DCTO	SANS a designar		europa	EU	01/11/2024	40	6	1	CIV - SUP NIVEL 18	7 200,00 €	PRR C19	7 200,00 €	500,00 €	1 000,00 €	25,00 €	375,27 €	9 100,27 €	1	
CNCS/PRR/PF2024/49	DDI	C-Aacdemy		TBD	PT-CONT	01/05/2024		5	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	300,00 €	0,00 €	250,10 €	630,10 €	1	
CNCS/PRR/PF2024/50	DDI	CIS		TBD	PT-CONT	01/07/2024		3	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	150,00 €	0,00 €	150,06 €	380,06 €	1	
CNCS/PRR/PF2024/51	DDI	CIS		TBD	PT-CONT	01/07/2024		3	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	150,00 €	0,00 €	150,06 €	380,06 €	1	
CNCS/PRR/PF2024/52	DDI	Comunicação e Imagem		TBD	PT-CONT	03/05/2024		5	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	300,00 €	0,00 €	250,10 €	630,10 €	1	
CNCS/PRR/PF2024/53	DDI	Observatório		TBD	PT-CONT	05/09/2024		3	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	150,00 €	0,00 €	150,06 €	380,06 €	1	
CNCS/PRR/PF2024/54	DDI	CIS		TBD	PT-CONT	05/09/2024		5	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	300,00 €	0,00 €	250,10 €	630,10 €	1	
CNCS/PRR/PF2024/55	DDI	Comunicação e Imagem		TBD	PT-CONT	07/10/2024		5	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	300,00 €	0,00 €	250,10 €	630,10 €	1	
CNCS/PRR/PF2024/56	DDI	Observatório		TBD	PT-CONT	07/10/2024		5	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	300,00 €	0,00 €	250,10 €	630,10 €	1	
CNCS/PRR/PF2024/57	DDI	Formação, Sensibilização e Treino		TBD	PT-CONT	07/05/2024		5	1	CIV - SUP NIVEL 18	0,00 €	PRR C19	0,00 €	80,00 €	300,00 €	0,00 €	250,10 €	630,10 €	1	
													331 250,00 €	**21 620,00 €**	**26 950,00 €**	**580,00 €**	**13 020,85 €**	**393 420,85 €**		
															Transp. + Estadas	**49 150,00 €**				

ANEXO C - QUAR

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

António José Gameiro Marques
Digitally signed by António José Gameiro Marques
Date: 2024.04.03 16:30:57 +01'00'

Data: 03/04/2024

Versão: V1

Ciclo de Gestão:	**01-01-2024 a 31-12-2024**
Designação do Serviço|Organismo:	**GABINETE NACIONAL DE SEGURANÇA**
Missão:	**A sua MISSÃO, nos termos do n.º 1 do artigo 2.º do Decreto-Lei n.º 3/2012 de 16 de Janeiro, republicado pelo Decreto-Lei nº 136/2017, de 06 de novembro e alterado pelo Decreto-Lei n.º 139-A/2023, de 29 de dezembro, é "(...) garantir a segurança da informação classificada 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..." e "...contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, ..."**

Objetivos Estratégicos (OE)		Meta	Grau de concretização
OE 1:	**Robustecer a capacidade de conhecimento do ciberespaço para a proteção da sociedade.**	80,00%	
OE 2:	**Desenvolver competências na área da informação classificada que contribuam para uma melhor resposta às necessidades emergentes.**	75,00%	
OE 3:	**Consolidar a qualidade da prestação de serviços.**	70,00%	
OE 4:	**Investir na formação e no bem-estar das pessoas trabalhadoras.**	90,00%	

Objetivos Operacionais (OP)

EFICÁCIA

Ponderação: 30%

OE1	OP1: Apresentar o projeto de regulamento relativo à implementação do RJSC na Administração Pública										Peso:	60%
Indicadores		**N-3 Resultado**	**N-2 Resultado**	**Última Monitorização N-1**	**Meta N**	**Tolerância**	**Valor Crítico**	**Peso**	**Resultado**	**Taxa de Realização**	**Classificação**	**Desvio**
Ind. 1	Enviar para a Tutela o projeto de Regulamento Jurídico do Ciberespaço (RJSC).				151	15	120	100%				
											Grau de Realização do OP1	

OE2	OP2: Desenvolver novas funcionalidades e melhorias do sistema de Credenciações online (CRESO+)										Peso:	40%
Indicadores		**N-3 Resultado**	**N-2 Resultado**	**Última Monitorização N-1**	**Meta N**	**Tolerância**	**Valor Crítico**	**Peso**	**Resultado**	**Taxa de Realização**	**Classificação**	**Desvio**
Ind. 2	Taxa de execução da implementação das novas funcionalidades				80,00%	10,00%	100,00%	100%				
											Grau de Realização do OP2	

EFICIÊNCIA

Ponderação: 30%

OE3	OP3: Desenvolver um Sistema de Gestão e Controlo da Atividade Inspetiva e de Auditoria (GAIA)										Peso:	60%
Indicadores		N-3 Resultado	N-2 Resultado	Última Monitorização N-1	Meta N	Tolerância	Valor Crítico	Peso	Resultado	Taxa de Realização	Classificação	Desvio
Ind. 3	Percentagem de implementação do projeto GAIA				80,00%	10,00%	100,00%	50%				
											Grau de Realização do OP3	

OE3	OP4: Migrar os sistemas prioritários baseados em LINUX para versões atualizadas do sistema operativo										Peso:	40%
Indicadores		N-3 Resultado	N-2 Resultado	Última Monitorização N-1	Meta N	Tolerância	Valor Crítico	Peso	Resultado	Taxa de Realização	Classificação	Desvio
Ind. 4	Data de entrada dos serviços em produção				181,00	20,00	150,00	50%				
											Grau de Realização do OP4	

QUALIDADE

Ponderação: 40%

OE4	OP5: Promover a motivação das pessoas trabalhadoras do GNS/CNCS e melhorar a satisfação dos seus clientes										Peso:	100%
Indicadores		N-3 Resultado	N-2 Resultado	Última Monitorização N-1	Meta N	Tolerância	Valor Crítico	Peso	Resultado	Taxa de Realização	Classificação	Desvio
Ind.5	Número de atividades *team building* realizadas pelas pessoas trabalhadoras do GNS/CNCS				3,00	1,00	5,00	50%				
Ind.6	Grau de satisfação das pessoas trabalhadoras do GNS/CNCS e dos respetivos clientes				70,00%	10,00%	100,00%	50%				
											Grau de Realização do OP5	

AVALIAÇÃO FINAL DO QUAR				
Avaliação de acordo com os requisitos previstos no artigo 18.º da Lei n.º 66-B/2007, de 28 de dezembro	**Âmbito**	**Eficácia Ponderação: 30%**	**Eficiência Ponderação : 30%**	**Qualidade Ponderação : 40%**
	Quantitativa	***0%***		
	Qualitativa	***Desempenho BOM; SATISFATÓRIO; INSUFICIENTE***		

Grau de realização Parâmetros e Objetivos							
Objetivos Operacionais	**Peso dos parâmetros na avaliação final**	**Peso dos objetivos no respetivo parâmetro**	**Peso de cada objetivo na avaliação final**	**Grau de realização do objetivo**	**Grau de realização do objetivo *(ponderado)***	**Classificação**	**OBJETIVOS MAIS RELEVANTES (nº 1 do art.18º da Lei 66-B/2007, de 28.12)**
EFICÁCIA	**0,0%**						
OP1: Apresentar o projeto de regulamento relativo à implementação do RJSC na Administração Pública	**30%**	**60%**	**18%**				**RELEVANTE**
OP2: Desenvolver novas funcionalidades e melhorias do sistema de Credenciações online (CRESO+)		**40%**	**12%**				
EFICIÊNCIA	**0,0%**						
OP3: Desenvolver um Sistema de Gestão e Controlo da Atividade Inspetiva e de Auditoria (GAIA)	**30%**	**60%**	**18%**				**RELEVANTE**
OP4: Migrar os sistemas prioritários baseados em LINUX para versões atualizadas do sistema operativo		**40%**	**12%**				
QUALIDADE	**0,0%**						
OP5: Promover a motivação das pessoas trabalhadoras do GNS/CNCS e melhorar a satisfação dos seus clientes	**40%**	**100%**	**40%**				**RELEVANTE**
Total	**100%**	**Soma dos pesos dos objetivos operacionais mais relevantes**					**76%**

RECURSOS HUIMANOS										Dias úteis de N	228
DESIGNAÇÃO	Pontuação (Conselho Coordenador da Avaliação de Serviços)	Pontuação efetivos Planeados para N			Pontuação efetivos Executados em N			Desvio (em n.º)	Pontuação Executada / Pontuação Planeada		UERHE / UERHP
		N.º de efetivos planeados (Mapa de Pessoal)	UERHP	Pontuação Planeada	N.º de efetivos a 31.dez (Balanço Social)	UERHE	Pontuação Executada				
Dirigentes - Direção Superior	20	3	684	60		0	0	-3	0%		0%
Dirigentes - Direção Intermédia e Chefes de equipa	16	13	2964	208		0	0	-13	0%		0%
Outros Oficiais	12	19	4332	228		0	0	-19	0%		0%
Sargentos	8	32	7296	256		0	0	-32	0%		0%
Praças ou Agentes da PSP	5	13	2964	65		0	0	-13	0%		0%
Técnicos Superiores ou Consultores	12	15	3420	180		0	0	-15	0%		0%
Técnico	12	55	12540	660		0	0	-55	0%		0%
Assistente Técnico	8	4	912	32		0	0	-4	0%		0%
Assistente Operacional	5	2	456	10		0	0	-2	0%		0%
Total		156	35 568	1 699	0	0	0	-156	0%		0%

Número de trabalhadores a exercer funções no serviço:	Efetivos 31.12.n-5	Efetivos 31.12.n-4	Efetivos 31.12.n-3	Efetivos 31.12.n-2	Previstos n-1	Efetivos 31.12.n-1	Previsto n	Efetivos 30.06.n	Efetivos 30.09.n	Efetivos 30.12.n
	99	106	113	108	100	122	156			-156

RECURSOS FINANCEIROS							
DESIGNAÇÃO	Dotação Inicial	Dotação Corrigida	Execução			Saldo	Taxa de execução
			30.06.n	30.09.n	31.12.n		
Orçamento de Funcionamento (OF)	**6 411 900,00 €**	**250,00 €**	**40,00 €**	**120,00 €**	**160,00 €**	**90,00 €**	**64%**
Despesas c/ Pessoal	4 012 150,00 €	50,00 €	10,00 €	30,00 €	10,00 €	40,00 €	20%
Aquisições de Bens e Serviços	1 633 891,00 €	50,00 €	10,00 €	30,00 €	50,00 €	0,00 €	100%
Outras despesas correntes	39 523,00 €	100,00 €	10,00 €	30,00 €	50,00 €	50,00 €	50%
Despesas de Capital	726 336,00 €	50,00 €	10,00 €	30,00 €	50,00 €	0,00 €	100%
Orçamento de Investimento (OI)	**17 070 454,00 €**	**250,00 €**	**40,00 €**	**120,00 €**	**160,00 €**	**90,00 €**	**64%**
Despesas c/ Pessoal	84 915,00 €	50,00 €	10,00 €	30,00 €	10,00 €	40,00 €	20%
Aquisições de Bens e Serviços	6 191 875,00 €	50,00 €	10,00 €	30,00 €	50,00 €	0,00 €	100%
Outras despesas correntes		100,00 €	10,00 €	30,00 €	50,00 €	50,00 €	50%
Despesas de Capital	10 793 664,00 €	50,00 €	10,00 €	30,00 €	50,00 €	0,00 €	100%
Outras despesas		**100,00 €**	**100,00 €**	**100,00 €**	**35,00 €**	**100,00 €**	**35%**
Total (OF+OI+OD)	**23 482 354,00 €**	**600,00 €**	**180,00 €**	**340,00 €**	**355,00 €**	**280,00 €**	**59%**

Ref.º.	Descritivo	Unidade(s) Orgânica(s) Responsável(eis)	Fórmula de cálculo	Fonte de Verificação	Justificação do Valor Crítico
Ind1	Enviar para a Tutela o projeto de Regulamento Jurídico do Ciberespaço (RJSC).	CNCS/DRSC	∑ do n.º de dias até ao envio para a tutela	Email de cobertura comprovativo do envio do regulamento	Corresponde à ambição máxima subjacente ao indicador ié, o cumprimento na transposição da diretiva (EU) 2022/2555 no prazo estabelecido. O cálculo de dias considera a data de início de 01 de janeiro 2024 e a data de fim, 31 de maio de 2024.
Ind2	Taxa de execução da implementação das novas funcionalidades	GNS/NAD	Racio das novas funcionalidades implementadas sobre a totalidade das funcionalidades propostas	Plano de implementação	Valor máximo teoricamente possível (100%).
Ind3	Percentagem de implementação do projeto GAIA	GNS/DIA	Racio das funcionalidades implementadas sobre a totalidade das funcionalidades propostas no plano	Plano de Desenvolvimento e Implementação	Valor máximo teoricamente possível (100%).
Ind4	Data de entrada dos serviços em produção	CNCS/DST	∑ do n.º de dias até à entrada em produção dos serviços	Notificação por email da entrada ao serviço do novo sistema operativo	Corresponde à ambição máxima subjacente ao indicador. O cálculo de dias considera a data de início de 01 de janeiro 2024 e a data de fim, 31 de maio de 2024.
Ind5	Número de atividades team building realizadas pelas pessoas trabalhadoras do GNS/CNCS	GNS/NAD	∑ do n.º de atividades realizadas	Convocatórias para as respetivas atividades	Corresponde à ambição máxima subjacente ao indicador. (Nº de atividades realizadas)
Ind6	Grau de satisfação das pessoas trabalhadoras do GNS/CNCS e dos respetivos clientes	GNS/NAD	Taxa de satisfação	Resultado das respostas aos inquéritos interno e externo	Considerando que é aplicado pela 1ª vez o questionário de satisfação, a entidade ambiciona 70%.

NOTAS EXPLICATIVAS:

ANEXO D – PROPOSTA DE ORÇAMENTO

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

Visto
O Diretor-Geral
António José Gameiro Marques
Digitally signed by António José Gameiro Marques
Date: 2024.04.04 15:02:55 +01'00'

GABINETE NACIONAL DE SEGURANÇA

ORÇAMENTO DE DESPESA - PROJETOS

Programa	Medida	Funcional	Fonte de Financiamento	Classificação Económica		Ativ	Proposta OE2024
PT SIC VIII							
2	1	1013	357	D.02.02.20.E0.00	Outros trabalhos especializados - Outros	PTSIC VIII	**154 000 €**
2	1	1013	357	D.02.02.13.00.00	Deslocaçoes e Estadas		**11 100 €**
2	1	1013	482	D.02.02.20.E0.A0	Outros trabalhos especializados - Outros		**154 000 €**
2	1	1013	482	D.02.02.13.00.00	Deslocaçoes e Estadas		**11 100 €**
PTQCI - Portuguese Quantum Communications Infrastructure							
2	1	1013	482	D.07.01.07.A0.C0	Outros	PTQCI	**248 435 €**
NCC - Centro Nacional de Coordenação							
2	1	1013	357	D.07.01.07.A0.C0	Outros	NCC	**3 750 €**
2	1	1013	482	D.07.01.07.A0.C0	Outros		**3 750 €**
2	1	1013	357	D.02.02.13.00.00	Deslocaçoes e Estadas		**9 750 €**
2	1	1013	357	D.02.02.14.A0.00	Serviços de Natureza Informática		**10 750 €**
2	1	1013	357	D.02.02.16.00.00	Seminários e Exposições		**6 750 €**
2	1	1013	357	D.02.02.20.A0.C0	Out trab Espec - Serv Natur Informática - Outros		**52 000 €**
2	1	1013	482	D.02.02.13.00.00	Deslocaçoes e Estadas		**9 750 €**
2	1	1013	482	D.02.02.14.A0.00	Estudos, Parec. Proj. e Consult - Serv Natureza Informática		**10 750 €**
2	1	1013	482	D.02.02.16.00.00	Seminários e Exposições		**6 750 €**
2	1	1013	482	D.02.02.20.A0.C0	Out trab Espec - Serv Natur Informática - Outros		**52 000 €**
C-Hub - Polo de Inovação Digital em Cibersegurança							
2	1	1013	357	D.02.02.13.00.00	Deslocaçoes e Estadas	C-HUB	**8 900 €**
2	1	1013	357	D.02.02.15.00.00	Formação		**6 100 €**
2	1	1013	357	D.02.02.20.A0.A0	Outros trabalhos especializados - Desenv Software		**17 900 €**
2	1	1013	48B	D.02.02.13.00.00	Deslocaçoes e Estadas		**8 900 €**
2	1	1013	48B	D.02.02.15.00.00	Formação		**18 500 €**
2	1	1013	48B	D.02.02.20.A0.A0	Outros trabalhos especializados - Desenv Software		**53 500 €**
12653 - Investimento TD-C19-i03 - Projeto 4 - Criar as condições físicas e tecnológicas para a implementação e operacionalização do novo modelo de coordenação da cibersegurança e da segurança da informação.							
2	102	1016	483	D.01.01.03.A0.00	Pessoal dos Quadros - Regime de Função Publica		**14 106 €**
2	102	1016	483	D.01.01.13.A0.00	Subsidio de Refeição - Pessoal em Funções		**1 452 €**
2	102	1016	483	D.01.01.14.SF.A0	Subsidio de Férias - Pessoal em Funções		**1 176 €**
2	102	1016	483	D.01.01.14.SN.A0	Subsidio de Natal - Pessoal em Funçoes		**1 176 €**
2	102	1016	483	D.01.03.05.A0.B0	Segurança Social		**3 911 €**

2	102	1016	483	D.02.02.14.D0.00	Outros		**40 000 €**
2	102	1016	484	D.02.02.14.D0.00	Outros	12653	**9 200 €**
2	102	1016	483	D.07.01.03.A0.B0	Conservação ou Reparação		**4 200 000 €**
2	102	1016	483	D.07.01.07.A0.C0	Outros		**300 000 €**
2	102	1016	483	D.07.01.09.A0.B0	Outros		**200 000 €**
2	102	1016	484	D.07.01.03.A0.B0	Conservação ou Reparação		**944 179 €**
2	102	1016	484	D.07.01.07.A0.C0	Outros		**69 000 €**
2	102	1016	484	D.07.01.09.A0.B0	Outros		**46 000 €**
12650 - PROJETO PT SIC VII							
2	1	1013	357	D.02.02.20.A0.C0	Out trab Espec - Serv Natur Informática - Outros	12650	**31 000 €**
12425 - Investimento TD-C19-i03 - Projeto 3 - Implementar o quadro nacional de cibersegurança e transformar o atual modelo de coordenação da cibersegurança e da segurança da informação							
2	102	1016	483	D.02.02.09.A0.00	Acessos à Internet		**2 000 €**
2	102	1016	483	D.02.02.14.D0.00	Outros		**163 000 €**
2	102	1016	483	D.02.02.15.B0.00	Outras		**280 000 €**
2	102	1016	483	D.02.02.20.E0.00	Outros		**980 000 €**
2	102	1016	484	D.02.02.09.A0.00	Acessos à Internet		**460 €**
2	102	1016	484	D.02.02.14.D0.00	Outros		**37 490 €**
2	102	1016	484	D.02.02.15.B0.00	Outras		**64 400 €**
2	102	1016	484	D.02.02.20.E0.00	Outros	12425	**225 400 €**
2	102	1016	483	D.07.01.03.A0.B0	Conservação ou Reparação		**180 000 €**
2	102	1016	483	D.07.01.07.A0.C0	Outros		**1 750 000 €**
2	102	1016	483	D.07.01.08.A0.B0	Outros		**690 000 €**
2	102	1016	484	D.07.01.03.A0.B0	Conservação ou Reparação		**41 400 €**
2	102	1016	484	D.07.01.07.A0.C0	Outros		**402 500 €**
2	102	1016	484	D.07.01.08.A0.B0	Outros		**158 700 €**
12410 - Investimento TD-C19-i03 - Projeto 2 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação							
2	102	1016	483	D.02.02.14.D0.00	Outros		**50 000 €**
2	102	1016	483	D.02.02.15.B0.00	Outras		**45 000 €**
2	102	1016	483	D.02.02.20.E0.00	Outros		**308 727 €**
2	102	1016	484	D.02.02.14.D0.00	Outros		**11 500 €**
2	102	1016	484	D.02.02.15.B0.00	Outras		**10 350 €**
2	102	1016	484	D.02.02.20.E0.00	Outros		**80 500 €**
2	102	1016	483	D.01.01.03.A0.00	Pessoal dos Quadros - Regime de Função Publica		**27 580 €**
2	102	1016	483	D.01.01.13.A0.00	Subsidio de Refeição - Pessoal em Funções		**1 452 €**
2	102	1016	483	D.01.01.14.SF.A0	Subsidio de Férias - Pessoal em Funções	12410	**2 299 €**
2	102	1016	483	D.01.01.14.SN.A0	Subsidio de Natal - Pessoal em Funçoes		**2 299 €**
2	102	1016	483	D.01.03.05.A0.B0	Segurança Social		**7 643 €**
2	102	1016	483	D.07.01.07.A0.C0	Outros		**245 000 €**
2	102	1016	483	D.07.01.08.A0.B0	Outros		**175 000 €**
2	102	1016	483	D.07.01.10.A0.B0	Outros		**750 000 €**
2	102	1016	484	D.07.01.07.A0.C0	Outros		**56 350 €**
2	102	1016	484	D.07.01.08.A0.B0	Outros		**40 250 €**
2	102	1016	484	D.07.01.10.A0.B0	Outros		**172 500 €**
12402 - Investimento TD-C19-i03 - Projeto 1 - Reforçar a capacitação em cibersegurança e segurança da informação							
2	102	1016	483	D.02.02.09.A0.00	Acessos à Internet		**5 000 €**
2	102	1016	483	D.02.02.15.B0.00	Outras		**210 000 €**

2	102	1016	483	D.02.02.16.00.00	Seminários, Exposições e Similares		**160 000 €**
2	102	1016	483	D.02.02.20.E0.00	Outros		**2 263 479 €**
2	102	1016	484	D.02.02.09.A0.00	Acessos à Internet		**1 150 €**
2	102	1016	484	D.02.02.15.B0.00	Outras		**48 300 €**
2	102	1016	484	D.02.02.16.00.00	Seminários, Exposições e Similares		**36 800 €**
2	102	1016	484	D.02.02.20.E0.00	Outros		**525 619 €**
2	102	1016	483	D.01.01.03.A0.00	Pessoal dos Quadros - Regime de Função Publica	12402	**14 106 €**
2	102	1016	483	D.01.01.13.A0.00	Subsidio de Refeição - Pessoal em Funções		**1 452 €**
2	102	1016	483	D.01.01.14.SF.A0	Subsidio de Férias - Pessoal em Funções		**1 176 €**
2	102	1016	483	D.01.01.14.SN.A0	Subsidio de Natal - Pessoal em Funçoes		**1 176 €**
2	102	1016	483	D.01.03.05.A0.B0	Segurança Social		**3 911 €**
2	102	1016	483	D.07.01.07.A0.C0	Outros		**90 600 €**
2	102	1016	483	D.07.01.08.A0.B0	Outros		**4 400 €**
2	102	1016	484	D.07.01.07.A0.C0	Outros		**20 838 €**
2	102	1016	484	D.07.01.08.A0.B0	Outros		**1 012 €**

	TOTAL	**17 070 454 €**

ANEXO E – MAPA DE PESSOAL

PÁGINA DEIXADA EM BRANCO

Mapa de Pessoal do Gabinete Nacional de Segurança e Centro Nacional de Cibersegurança - 2024

Artigo 29º LTFP

VISTO
(O Dirigente Máximo))

António José Gameiro Marques
Digitally signed by António José Gameiro Marques
Date: 2023.08.10 19:17:18 +01'00'

APROVO
(Membro do Governo)

Mário Campolargo

Assinado de forma digital por Mário Campolargo
DN: c=PT, title=Secretário de Estado, o=Gabinete do Secretário de Estado da Digitalização e da Modernização Administrativa, ou=Campolargo, givenName=Mário, cn=Mário Campolargo
Dados: 2023.08.17 22:42:58 +01'00'

Unidade Orgância	Atribuições / competências / atividades	Base legal	Cargos / carreiras / categorias										Nº de postos de trabalho	
			Cargos de Direção Superior e Intermédia				Cargos Civis			Cargos Militares das Forças Armadas ou das Forças de Segurança (*)				
			Diretor geral	Subdiretor geral	Chefe de Equipa Multidisciplinar (Civil)	Chefe de Equipa Multidisciplinar (Militar) (*)	Tecnico Superior ou Consultor	Assistente Técnico ou Técnico (CNCS)	Assistente Operacional	Oficial	Sargento ou Chefe (PSP)	Praça ou Agente (PSP)	Ocupados e/ou a ocupar em 2023	Necessários para assegurar atribuições 2024
Direção Comum GNS + CNCS	Direção		1										1	1
	Secretária/o							1					1	1
	Motorista (**)											1	1	1
	Subtotal		**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0**	**1**	**3**	**3**
Direção do GNS e Nucleo de Apoio à Direção	Direção			1									1	1
	Assessor ou Adjunto de Direção					1	2			3			6	6
	Oficial de Segurança									1			1	1
	Segurança de Instalações											2	2	2
	Motorista (**)											1	1	1
	Subtotal		**0**	**1**	**0**	**1**	**2**	**0**	**0**	**4**	**0**	**3**	**11**	**11**
Equipas Multidisciplinares	Chefe de equipa					7							7	7
	Adjuntos						4			15			17	19
	Técnicos							2			32	9	42	43
	Motorista								1				1	1
	Assistente Operacional								1				1	1
	Subtotal		**0**	**0**	**0**	**7**	**4**	**2**	**2**	**15**	**32**	**9**	**68**	**71**
Centro Nacional de Cibersegurança	Direção			1									1	1
	Consultor Coordenador				5								5	5
	Consultor						9						9	9
	Técnico							55					24	55
	Secretária/o							1					1	1
	Subtotal		**0**	**1**	**5**	**0**	**9**	**56**	**0**	**0**	**0**	**0**	**40**	**71**
TOTAL GERAL			**1**	**2**	**5**	**8**	**15**	**59**	**2**	**19**	**32**	**13**	**122**	**156**

Notas explicativas:

(*) Em conformidade com o estipulado no nº 3 do artigo 6º do Decreto-Lei nº 3/2012, de 16 de janeiro, na sua redação atual, os postos de trabalho são preenchidos com elementosdos quadros das Forças Armadas e Serviços de Segurança (atualmente sem impacto orçamental no GNS, uma vez que os vencimentos e abonos são assegurados pelas entidades das quais são oriundos, os ramos das Forças Armadas, a GNR e a PSP), excepto ajudas de custo, suplemento de risco e despesas de representação.

(**) Os dois motoristas indicados são elementos das Forças Armadas - Marinha, atribuídos ao DG e SDG GNS, por serem oficiais generais desse Ramo - só oneram o OE pelo abono do suplemento de risco

Os 33 novos postos de trabalho forma aprovados por Despacho Interno n.º 110/2023/MF do Ministro das Finanças , exarado sobre o Despacho n.º 368/2023/SEO da Secretária de estado do Orçamento:

1 Consultor no GNS, para a Equipa Multidisciplinar de Informática, Redes e Comunicações permitindo reforçar e capacitar esta equipa por forma a assegurar a continuidade e persistência do conhecimento sobre os sistemas de informação críticos do GNS (CRESO, eSEIF, SCRITO E GAIA)

1 posto de trabalho na categoria de Técnico Superior no GNS, através de mobilidade efutura consolidação, para reforçar a Equipa Multidisciplinar de Administração e Logística;

31 postos de trabalho a afetar ao CNCS, todos na categoria de Técnico, a prover em comissão de serviço nos termos do n.º 7 do artigo 6.º-A do Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual, conferida pelo Decreto-Lei n.º 136/2017, de 6 de novembro.

NOTA:

No âmbito do Despacho 11888-B/2021, de 30 de novembro, o GNS tem um contigente de 3 posto de trabalho para a constituição de vínculo de emprego público (comissão de serviço) pelo período máximo de execução dos projetos PRR e que sejam integralmente suportados pelo PRR

ANEXO F – CÓDIGO DE ÉTICA E CONDUTA

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

PÁGINA DEIXADA EM BRANCO

PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança

CÓDIGO ÉTICA E CONDUTA
do GNS

GNS Gabinete Nacional de Segurança PORTUGAL

Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

CONTROLO DO DOCUMENTO

Versão	Data de Elaboração	Data de Aprovação	Descrição
N.º 1	16/07/2018	16/07/2018	Código de Ética e Conduta do GNS-CNCS
N.º 2	26/05/2022		Código de Ética e Conduta do GNS-CNCS

Gabinete Nacional de Segurança

Rua da Junqueira, 69 1300-342 Lisboa

Telefone: 21 040 36 00

Fax: 21 040 36 98

E-mail: geral@gns.gov.pt

PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança

CÓDIGO ÉTICA E CONDUTA do GNC-CNCS

1.ª Edição

Disponível em: Outubro 2022

GNS Gabinete Nacional de Segurança PORTUGAL

Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Índice

Mensagem do Diretor-Geral

O Código de Conduta é um instrumento da maior importância, representando, a nível do Gabinete Nacional de Segurança (GNS) e do Centro Nacional de Cibersegurança (CNCS), um compromisso empenhado, interno e externo, na prossecução dos mais elevados valores éticos, assentes em princípios de atuação que valorizam a honestidade, integridade, lealdade, solidariedade, rigor e honra.

O Código de Conduta reflete também a nossa visão de que o relacionamento com todos os nossos públicos de interesse deverá assentar em fortes pilares de profissionalismo, rigor, confiança e segurança, sendo estes atributos importantes para a nossa identidade.

Tenho a forte convicção de que o Código de Conduta contribuirá para que consigamos fortalecer cada vez mais a nossa cultura organizacional e a disseminação junto dos(as) nossos(as) Colaboradores(as) dos mais elevados padrões éticos, contribuindo positivamente para a afirmação e reputação do GNS e do CNCS junto das Forças Armadas, Forças de Segurança, Administração Pública, do mundo empresarial e da sociedade em geral.

Este documento é, pois, um compromisso de todos e cada um(a) dos(as) colaboradores(as) perante o GNS/ CNCS e a sociedade. É um elemento de fulcral importância, a juntar à nossa Missão, Visão e Valores.

Os princípios e procedimentos neles presentes devem ser respeitados e assumidos.

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2022.10.26 17:33:46 +01'00'

O Diretor-geral

António Gameiro Marques

CALM

1. Nota Introdutória

O Código de Conduta do Governo, através da Resolução do Conselho de Ministros n.º 42/2022, de 9 de maio, estabelece os princípios e critérios orientadores respeitantes à conduta dos membros do Governo, dos membros dos Gabinetes e do Dirigentes Superiores da Administração Pública sob a direção do Governo, bem como dos dirigentes e gestores de institutos e de empresas públicas, como forma de assegurar a transparência e o controlo da integridade do sistema democrático, promovendo a confiança dos cidadãos nas instituições do Estado de Direito.

Nesta revisão do Código de Conduta do Gabinete Nacional de Segurança, pretende-se ir ao encontro das medidas de prevenção de conflitos de interesse previstas na Estratégia Nacional Anticorrupção 2020-2024, aprovada pela Resolução do Conselho de Ministros n.º 37/2021, de 6 de abril, materializadas no regime geral de prevenção da corrupção, aprovado em anexo ao Decreto-lei n.º 109-E/2021, de 9 de dezembro e onde o código de conduta surge como instrumento central para estabelecer o conjunto de princípios, valores e regras de atuação em matéria de ética no exercício de funções no setor público, privado ou cooperativo.

Neste desígnio, o Código de Ética e de Conduta do GNS é um instrumento de enquadramento e apoio à ação, que se pretende dinâmico, através do qual se estabelece um conjunto de princípios e de regras de natureza ética e deontológica que deve presidir ao cumprimento das atividades desenvolvidas pelo GNS/CNCS, quer no âmbito da prossecução da sua missão, quer no exercício das atividades que lhe servem de suporte, a que os colaboradores se encontram sujeitos e que devem assumir como intrinsecamente seus, refletindo-os na relação profissional que estabelecem entre si e com terceiros.

Em particular, o Código de Ética e de Conduta inclui informação e procedimentos sobre normas de condutas, designadamente no que se refere a situações de conflito de interesse, sigilo profissional e tratamento de informação privilegiada, acumulação de funções e deteção e comunicação de fraude e corrupção.

2. Âmbito de Aplicação

O presente Código de Conduta aplica-se a todos os colaboradores do GNS/CNCS, independentemente da natureza das funções e do respetivo vínculo jurídico.

Todos os colaboradores devem comprometer-se à escrupulosa observância do Código de Conduta, pautando a sua atuação por comportamentos eticamente sustentados, não devendo, em circunstância alguma, negligenciar o impacte que as suas decisões, formas de atuação e comportamentos, por ação ou omissão, possam ter na relação profissional que estabelecem entre si e com terceiros.

Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

A aplicação do Código de Conduta e o seu cumprimento não impede, substitui ou afasta a aplicação obrigatória de legislação aplicável, e bem assim de outros códigos, regulamentos ou manuais internos do GNS/CNCS.

3. Referenciais

Constituem referenciais do presente Código de Conduta a Declaração Universal dos Direitos do Homem, a Constituição da República Portuguesa, a Lei nº 73/2017 de 16 de agosto que reforça o quadro legislativo para a prevenção da prática de assédio[1], à Legislação Laboral, os Princípios Éticos da Administração Pública e a Resolução do Conselho de Ministros n.º 42/2022, de 9 de maio — Código de Conduta do Governo.

4. Missão

O GNS tem por missão garantir a Segurança da Informação Classificada 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 informação classificada, 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;

Exercer, em Portugal, os poderes públicos cometidos às autoridades nacionais de segurança, nomeadamente nas áreas da credenciação de segurança, segurança das comunicações, distribuição de informação classificada e outras, nos termos das normas aprovadas pelas entidades internacionais competentes;

Proceder ao registo, distribuição e controlo da informação classificada, 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, informação classificada sob responsabilidade portuguesa, dentro e fora do território nacional;

[1] Para além de proceder à décima segunda alteração ao Código do Trabalho, aprovado em anexo à Lei n.º 7/2009, de 12 de fevereiro, à sexta alteração à Lei Geral do Trabalho em Funções Públicas, aprovada em anexo à Lei n.º 35/2014, de 20 de junho, e à quinta alteração ao Código de Processo do Trabalho, aprovado pelo Decreto-Lei n.º 480/99, de 9 de novembro.

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;

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.

No âmbito do GNS funciona o Centro Nacional de Cibersegurança (CNCS), que tem por missão contribuir para que o País use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.

Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

5. Visão

O GNS pretende ser visto como uma organização altamente resiliente, combinando a capacidade para, no imediato, enfrentar os impactos de choques, mantendo uma alta Código de Conduta reputação percecionada pelos públicos de interesse no âmbito do cumprimento da missão institucional, com a capacidade para se adaptarem às condições da mudança constante, pensando como organizações que aprendem com vista à adaptação às novas realidades, e que inovam, procurando fazer diferente, criando novos produtos/serviços e métodos de trabalho, antecipando as necessidades/expectativas dos públicos de interesse.

Assim, a VISÃO do GNS/CNCS pode ser traduzida em:

"Contribuir para um Portugal mais seguro, através de um comportamento resiliente e de um pensamento inovador."

6. Valores

Lealdade: professada na prática da verdade, da fidelidade aos princípios éticos, e da constância e firmeza no compromisso assumido para com as chefias, para consigo e para com os seus pares. Pressupõe a confiança nas decisões dos superiores, no apoio dos pares ao esforço coletivo e no trabalho dos colaboradores.

Solidariedade: valor que nos conduz a partilhar momentos de sofrimento, de dificuldade e também de alegria com o próximo, consiste em dar e receber ajuda, sendo, por isso, um valor que exige um contexto social e uma perceção mais humana do próximo, tornando o espaço de trabalho mais agradável e assim mais propício à criação de valor. Facilita a construção de vínculos afetivos, contribui para o fortalecimento da autoestima, conduz a um sentimento de realização e satisfação pessoal e à criação de um forte espírito de equipa.

Honestidade: ato de ser honesto, de ser verdadeiro. É virtude que exige coerência e sinceridade no agir, sentir e falar.

Rigor: fazer com seriedade de princípios, exatidão, precisão, concisão e pontualidade.

Honra: percecionada na conduta virtuosa, na firmeza e na dignidade de carácter. Espelha honestidade, respeito e seriedade, e reflete-se no reconhecimento público que se obtém pelo cumprimento do dever, donde resulta reputação e prestígio.

Integridade: assunção de responsabilidades, materializada na transparência, honestidade e justeza das decisões e atos. Tem como retorno o respeito e a confiança dos outros.

7. Princípios Gerais

A atuação dos colaboradores do GNS/CNCS deve pautar-se por princípios de lealdade, isenção, rigor e transparência no contexto do cumprimento da sua missão, privilegiando as responsabilidades subjacentes à

prestação de serviço público e ao reforço de uma imagem de integridade e excelência, e evitando situações suscetíveis de originar conflitos de interesse.

São princípios gerais deste Código:

Princípio da Legalidade, Justiça e Imparcialidade

Os colaboradores do GNS/CNCS devem agir em obediência à lei e ao direito, com justiça, imparcialidade e isenção dentro dos limites das funções e competências que lhes estejam cometidas e devem adotar os comportamentos adequados aos fins prosseguidos, ficando impedidas práticas ou decisões arbitrárias e comportamentos que resultem em benefícios ou prejuízos ilegítimos.

Princípio da Colaboração e Boa-Fé

Os colaboradores do GNS-CNCS devem atuar com zelo, adequado espírito de cooperação e responsabilidade, informando e esclarecendo de forma respeitosa, clara e simples, todos os intervenientes, estimulando iniciativas e sugestões, preservando os valores de transparência e abertura, no relacionamento pessoal, independentemente da posição hierárquica ocupada, tendo em vista o adequado cumprimento dos objetivos que lhes são atribuídos.

Princípio da prossecução do interesse público

Os colaboradores do GNS-CNCS devem atuar com subordinação ao interesse público, atuando com elevada eficiência, economia, eficácia e competência técnica, no cumprimento dos normativos e orientações em vigor, na disponibilização da informação de forma verdadeira, concisa e atempada e demonstrando capacidade de iniciativa e diligência na resolução de problemas, promovendo assim a melhoria contínua dos padrões de qualidade dos serviços prestados e assegurando, por essa forma, o cumprimento integral da boa administração a que se encontram sujeitos.

Princípio da boa administração

No exercício das atividades, funções e competências, o colaborador do GNS/CNCS deve pautar-se por critérios de eficiência, economia e eficácia e cumprir com diligência e zelo todas as tarefas que lhes sejam cometidas, garantindo a observância de todas as normas legais e procedimentos internos, tendo em vista a prestação de serviços de elevada qualidade técnica e uma cultura de serviço público de excelência.

Princípio da igualdade

Os colaboradores do GNS/CNCS não podem privilegiar, beneficiar, prejudicar, privar de qualquer direito ou isentar de qualquer dever, ninguém em razão de ascendência, sexo, raça, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual, e devem demonstrar sensibilidade e respeito mútuo abstendo-se de qualquer comportamento ofensivo, bem como respeitar escrupulosamente o direito à reserva da intimidade da vida privada.

Princípio da Competência, Eficiência e Responsabilidade

Os colaboradores do GNS_CNCS devem cumprir sempre com zelo, isenção, rigor, eficiência e transparência as responsabilidades e deveres que lhes sejam cometidos. Devem estar conscientes da importância dos respetivos deveres e responsabilidades, ter em conta as expetativas de terceiros relativamente à sua conduta dentro de padrões genérica e socialmente aceites, e comportar-se de forma a manter e a reforçar a confiança das entidades, públicas e privadas, e dos cidadãos no GNS_CNCS contribuindo para o cumprimento eficaz e eticamente exemplar da missão do GNS-CNCS.

Princípio da dignidade da pessoa humana e integridade física e moral

A atuação dos colaboradores do GNS/CNCS deve pautar-se pelo respeito pela dignidade da pessoa humana e pela inviolabilidade da sua integridade física e moral, proibindo-se todo o comportamento abusivo, incluindo o assédio sexual ou psicológico, de conduta verbal ou física de humilhação, de coação ou de ameaça para os colaboradores e demais pessoas que se relacionem com o GNS/CNCS.

Princípio da solidariedade

Compete aos trabalhadores manter e promover entre si um comportamento solidário e cooperante, designadamente entre áreas de atividade e equipas de projeto multidisciplinares, e bem assim com a Política de Gestão Integrada do GNS/CNCS, devendo respeitar a legislação, a regulamentação nacional e comunitária e outros requisitos aplicáveis naquelas matérias. Os colaboradores do GNS-CNCS pautam a sua atuação pelo respeito e proteção do ambiente, numa ótica de desenvolvimento sustentado, controlo dos riscos para a segurança e saúde no trabalho e demais princípios da responsabilidade social.

Princípio da Informação e Qualidade

Os colaboradores do GNS-CNCS devem manter um sentido de rigor, clareza e cortesia na prestação de informações e/ou esclarecimentos a terceiros, os quais, observadas que sejam as normas legais em matéria

de acesso à informação e de proteção de dados, devem ser facultados prontamente e em tempo útil, suprimindo a prática de atos que dificultem a sua tramitação. Os colaboradores do GNS-CNCS na sua relação com terceiros somente devem exigir a informação indispensável ao adequado desempenho das suas funções.

Princípio da Lealdade e Cooperação

O conceito de lealdade para os colaboradores do GNS-CNCS implica não só o adequado desempenho das tarefas que lhes são atribuídas pelos seus superiores hierárquicos, como o cumprimento das instruções destes últimos, assim como o respeito pelos canais hierárquicos apropriados e superiormente definidos. Devem igualmente garantir a transparência e a capacidade de diálogo, consideradas adequadas no trato diário com superiores hierárquicos e outros colegas.

Os colaboradores do GNS-CNCS devem facultar entre si toda a informação ou conhecimento necessários ao desenvolvimento de atividades ou participação em tarefas. A não revelação a superiores hierárquicos e colegas das informações necessárias que possam afetar o andamento dos trabalhos, sobretudo com o intuito de obter vantagens pessoais, assim como o fornecimento de informações falsas, inexatas ou desnecessárias e a recusa em colaborar com os colegas, considera-se como comportamento inadequado e violador do princípio de lealdade e cooperação.

Os colaboradores do GNS-CNCS devem promover o bom relacionamento interpessoal, assente numa base de respeito pelo próximo e por forma a assegurar a existência de relações cordiais. Os princípios gerais referidos anteriormente devem evidenciar-se no relacionamento dos colaboradores do GNS-CNCS com todos e com todas as entidades, quer sejam públicas ou privadas.

Princípio da Integridade

Os colaboradores do GNS_CNCS devem agir em todas as situações de acordo com critérios consubstanciados numa conduta honesta, diligente, garantindo a verdade e devem abster-se de práticas que possam suscitar dúvidas quanto ao respeito pelos princípios éticos que regulam o seu comportamento.

Os colaboradores do GNS-CNCS devem prestar uma especial atenção a favores, convites, gestos de hospitalidade e situações de cumplicidade que possam induzir a criação de vantagens ilícitas ou constituir formas dissimuladas de corrupção.

Os colaboradores do GNS-CNCS não devem aceitar, quer para si próprios, quer em nome de outrem, presentes ou outras ofertas que possam influenciar, que visem influenciar, ou que possam ser interpretadas forma de influenciar o seu trabalho, e devem de imediato ponderar se a aceitação do presente ou da oferta pode influenciar a sua imparcialidade ou prejudicar a confiança depositada no GNS_CNCS, sendo que, em

caso de dúvida, deve consultar o seu responsável hierárquico. No entanto, sem prejuízo do estabelecido anteriormente, é possível aceitar a hospitalidade ou pequenos presentes que, devido ao seu valor e à sua natureza, se considerem dentro dos limites normais da cortesia. Entende-se como presentes de mera cortesia os que apresentam um valor simbólico ou comercialmente despiciendo. No que respeita a ofertas institucionais e hospitalidades dirigidas aos dirigentes do GNS-CNCS aplica-se o estabelecido pela Lei n.º 52/2019, de 31 de julho, sendo obrigatória a informação da aceitação de ofertas de bens materiais ou serviços de valor estimado superior a 150 euros, desde que sejam compatíveis com a natureza institucional ou com relevância da representação própria do cargo, que configurem uma conduta socialmente adequada e conforme aos usos e costumes.

8. Normas de Conduta

Neste âmbito, pretende-se estabelecer o padrão de conduta exigível aos colaboradores do GNS-CNCS nas relações entre eles e nas relações com terceiros, destacando-se as seguintes normas de conduta que devem regular os seus comportamentos e atitudes:

Conflito de Interesses

Considera-se que existe conflito de interesses 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 e 73º do Código do Procedimentos Administrativo.

Os 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.

Os colaboradores da GNS-CNCS não podem exercer qualquer atividade externa que interfira com as funções que desempenham na 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 e o rigor nas decisões administrativas e levar à presunção de existência de falta de imparcialidade da sua atuação, no exercício das suas atividades.

A resolução de conflitos de interesses deve respeitar escrupulosamente as disposições legais, regulamentares e contratuais aplicáveis.

Os 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, devem subscrever a declaração individualizada de inexistência de conflitos de Interesses, conforme o modelo constante em *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 em *Anexo II – Declaração de Conflito de Interesses.*

Deteção e Comunicação de Fraude ou Corrupção

Os colaboradores do GNS-CNCS na sua conduta, procedem de acordo com critérios de razoabilidade e prudência, e devem informar o seu superior hierárquico, ou, em função da natureza da matéria envolvida, outras entidades competentes, designadamente o Ministério Público, o Tribunal de Contas, a Inspeção-geral de Finanças - Autoridade de Auditoria, o Organismo Europeu de Luta Antifraude (OLAF) ou a Procuradoria Europeia, no respeito pelas respetivas atribuições, sempre que tomem conhecimento ou tiverem suspeitas fundadas da ocorrência de atividades de corrupção, ativa ou passiva, criminalidade económica e financeira, branqueamento de capitais, tráfico de influências, apropriação ilegítima de bens públicos, de administração danosa, peculato, participação económica em negócios, abuso de poder ou violação do dever de segredo, aquisição de imóveis ou valores mobiliários em consequência da obtenção ou utilização ilícitas de informação privilegiada no exercício de funções na Administração Pública, dando especial atenção a qualquer forma de pagamentos, favores e cumplicidades que possam induzir a criação de vantagens ilícitas, de acordo com o modelo constante em *Anexo III – Comunicação de situação específica de não conformidade ou potencial fraude.*

A eventual omissão do dever de denúncia ou participação pode gerar responsabilidade disciplinar e/ou penal.

Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

O colaborador do GNS-CNCS que comunicar ou impedir a realização de atividades ilícitas, não poderá ser, por esse facto, prejudicado a qualquer título.

Proteção de Dados Pessoais

Os colaboradores do GNS com acesso a dados pessoais ou envolvidos no tratamento dos mesmos devem respeitar as disposições legais relativas à proteção dos dados pessoais, incluindo a sua circulação, e agir em conformidade com o disposto na Política Interna de Dados Pessoais do GNS, aprovada a 25 de junho de 2018.

Independência

Os colaboradores da GNS-CNCS em todos os contactos com o exterior, devem atuar em conformidade com o princípio da independência, nomeadamente, não solicitando ou recebendo instruções de qualquer entidade organização ou pessoa alheia ao GNS/CNCS. O respeito deste princípio implica a recusa de ofertas, pagamentos ou outros benefícios que pelo seu custo, carácter reiterado ou exclusivo, possam conduzir os envolvidos ou terceiros a presumir que os deveres de isenção e independência se encontram comprometidos.

Acumulação de Funções

Os colaboradores da 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 da 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.

Sigilo Profissional

Os colaboradores da GNS/CNCS, mesmo depois de cessarem de funções neste organismo, estão sujeitos ao sigilo profissional, em particular nas matérias que, por virtude de decisão interna ou por força da legislação em vigor[2], não devam ser do conhecimento geral.

[2] Artigos 21.º a 24.º Lei Geral do Trabalho em Funções Públicas.

Os colaboradores da GNS/CNCS que tenham acesso a dados pessoais relativos a pessoas singulares ou coletivas, ou outra informação confidencial, por via do exercício das suas funções, devem abster-se de divulgar essa informação a pessoas alheias ao serviço, bem como a outros colaboradores que não necessitem dessa informação para o desempenho das suas funções, ou de a usar em proveito próprio ou de terceiros, sob pena de poderem ser responsabilizados civil e criminalmente pelo acesso ou utilização indevida.
As informações pessoais sobre os colaboradores estão sujeitas ao princípio da confidencialidade, apenas podendo ter acesso o próprio ou quem tenha como responsabilidade específica a sua guarda, manutenção ou tratamento da informação.

Informação Privilegiada

Os colaboradores da GNS/CNCS durante o exercício das suas funções, ou após suspensão ou cessação das mesmas, não podem disponibilizar nem utilizar, em proveito próprio ou de terceiros, direta ou indiretamente, as informações a que têm ou tenham tido acesso, no exercício de funções ou por causa delas, encontrando-se sujeitos a segredo e reserva nos termos previstos na legislação aplicável.
Sem prejuízo do disposto na lei quanto ao acesso aos documentos administrativos, qualquer informação solicitada por representantes dos meios de comunicação social e relativa à atividade desenvolvida pelo GNS/CNCS deve ser sempre prestada através do Diretor-Geral ou com a sua autorização prévia.

Papel dos Colaboradores na aplicação deste Código de Conduta

A adequada aplicação do presente Código de Conduta depende, acima de tudo, do profissionalismo, consciência e capacidade de discernimento dos colaboradores do GNS/CNCS. Em particular, os Dirigentes Superiores, Chefes de Departamento / Equipas Multidisciplinares e Consultores Coordenadores, que devem ter uma atuação exemplar no tocante à adesão aos princípios e regras estabelecidos no presente documento, bem como assegurar o seu cumprimento.

9. Boas Práticas

Os colaboradores do GNS/CNCS devem ainda observar as seguintes boas práticas de conduta no relacionamento externo e interno:

10. Disposições Gerais

Os colaboradores do GNS/CNCS estão vinculados ao disposto no presente Código.

A violação por qualquer colaborador desta entidade de normas de ética e conduta constantes do presente Código deverá ser reportada superiormente, podendo fazer incorrer o colaborador em causa, em responsabilidade disciplinar nos termos da legislação em vigor, aplicáveis às infrações praticadas.

11. Atualização e publicitação

O presente Código será objeto de atualização sempre que se revele existir matéria pertinente que contribua para o reforço dos seus objetivos, e poderá ser suscitada por qualquer colaborador, sendo objeto de aprovação por parte do Diretor Geral do GNS. As atualizações do presente Código também devem ser objeto de declaração individualizada de compromisso pelos colaboradores do GNS, de acordo com o modelo constante em anexo (Anexo IV − Declaração de Compromisso).

12. ANEXOS

Anexo I - Modelo de Declaração de Inexistência de Conflito de Interesses

Anexo II – Modelo de Declaração de Conflito de Interesses

Anexo III – Modelo de Comunicação de situação específica de não conformidade ou potencial fraude

Anexo I - Modelo de Declaração de Inexistência de Conflito de Interesses

Modelo

Declaração de Inexistência de Conflito de Interesses

Identificação do Processo/Ação/Investimento/Contrato

Eu, abaixo assinado(a), ……, a desempenhar funções na ……, declaro, sob compromisso de honra, que não me encontro em qualquer situação de conflito de interesses relativamente ao processo/ação/investimento/contrato acima identificado e à(s) entidade(s) nele(a) envolvidos(as), que coloque em causa a isenção, imparcialidade, independência e justiça da sua conduta, ou que possa causar dúvidas sobre a sua conduta.

Nesse âmbito, sem prejuízo de outras situações legalmente previstas, declaro que não me encontro, designadamente, numa das situações a seguir indicadas:

1) Ter exercido a qualquer título, funções na(s) entidade(s) envolvida(s) nos últimos três anos;
2) Ter prestado à(s) entidade(s) envolvidas, por si ou por interposta pessoa, em regime de trabalho autónomo ou subordinado, serviços que possam ser submetidos à sua apreciação ou decisão ou à de órgãos/serviços/pessoas colocados sob sua direta influência[3] no âmbito do processo/ação/investimento/contrato;
3) Ter participado em processo de decisão da(s) entidade(s) envolvida(s), ou prestado aconselhamento, que tenham repercussão no processo/ação/investimento/contrato, ou na matéria abordada no seu âmbito;
4) Ter intervindo em ato abrangido no processo/ação/investimento/contrato, pessoalmente, através de mandatário ou como mandatário;

[3] Consideram-se colocados sob direta influência do trabalhador, os órgãos ou serviços que: a) Estejam sujeitos ao seu poder de direção, superintendência ou tutela; b) Exerçam poderes por ele delegados ou subdelegados; c) Tenham sido por ele instituídos, ou relativamente a cujo titular tenha intervindo como representante do empregador público, para o fim específico de intervir nos procedimentos em causa; d) Sejam integrados, no todo ou em parte, por trabalhadores por ele designados; e) Cujo titular ou trabalhadores neles integrados tenham, há menos de um ano, sido beneficiados por qualquer vantagem remuneratória, ou obtido menção relativa à avaliação do seu desempenho, em cujo procedimento ele tenha tido intervenção; f) Com ele colaborem, em situação de paridade hierárquica, no âmbito do mesmo órgão ou serviço.

5) Ter pessoa familiar[4] ou pessoa próxima[5] a exercer funções, ou que tenha exercido funções durante o período objeto do processo/ação/investimento/contrato, nos corpos gerentes ou na gestão financeira da(s) entidade(s) envolvida(s) ou ainda noutra posição que possa ser relevante para o processo/ação/investimento/contrato;
6) Ter pessoa familiar ou pessoa próxima que interveio em ato abrangido no processo/ação/investimento/contrato;
7) Ter interesse pessoal, financeiro[6], partidário ou religioso ou outro relacionado com o processo/ação/investimento/contrato, seja esse interesse seu, de pessoa de quem seja representante ou gestor de negócios, ou de pessoa familiar ou de pessoa próxima;
8) Ter envolvimento ou ter pessoa familiar ou pessoa próxima envolvida em convite de emprego ou processo de recrutamento para a(s) entidade(s) envolvida(s);
9) Ter o responsável da(s) entidade(s) envolvida(s) feito participação disciplinar ou intentado ação judicial contra si ou contra seu familiar ou pessoa próxima;
10) Ter ele próprio ou o seu conjugue ou equiparado, parente ou afim em linha reta[7], crédito ou débito litigiosos com a(s) entidade(s) envolvidas ou com responsável pela mesma;
11) Haver intimidade ou inimizade entre si ou seu conjugue ou equiparado e o responsável da(s) entidade(s) envolvida(s), que o impeça de intervir no processo/ação/investimento/contrato de forma isenta, imparcial, independente e justa.

O(a) signatário(a) mais declara assumir, sob compromisso de honra, que, no caso de ocorrência superveniente de conflito de interesses, ou de essa ocorrência vir a ser do seu conhecimento, informará de imediato o seu superior hierárquico desse facto, antes de tomadas decisões, ou praticados atos ou celebrados contratos.

Nome do(a) colaborador(a)	
Cargo/Função e Categoria	

[4] Considera-se familiar o conjugue não separado de pessoa e bens ou pessoa que com ele viva em união de facto, parente ou afim em linha eta ou até ao 3.º grau da linha colateral.
[5] Considera-se pessoa próxima qualquer tutelado ou maior acompanhado por si, pessoa de quem seja representante, gestor de negócios ou mandatário, bem como pessoa ligada ao declarante por laços suficientemente fortes em termos de poder interferir no seu juízo profissional.
[6] Incluindo, designadamente, quando detenha uma participação em capital da(s) entidade(s), direta ou indiretamente, por si mesmo ou conjuntamente com familiar ou pessoa próxima.
[7] Consideram-se o seu cônjuge não separado de pessoa e bens ou pessoa que com ele viva em união de facto, e ascendentes e descendentes em qualquer grau, colaterais até ao segundo grau.

É aplicável à conduta do(a) colaborador(a) signatário(a), com as necessárias adaptações, o disposto nos artigos 69.º a 76.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, na redação atual.

Lisboa, …… de …… 20…

Assinatura

Anexo II – Modelo de Declaração de Conflito de Interesses

Modelo

Declaração de Conflito de Interesses

Eu, abaixo assinado(a), ……, a desempenhar funções na ……, solicito escusa do desempenho das funções que me estão atribuídas na minha atividade ……., por considerar que não estão totalmente reunidas as condições para a salvaguarda de ausência de conflito de interesses.

Lisboa, …… de …… 20…

Assinatura

Anexo III – Modelo de Comunicação de situação específica de não conformidade ou potencial fraude

Modelo

Comunicação de situação específica de não conformidade ou potencial fraude

Eu, abaixo assinado(a), ……, a desempenhar funções na ……, informo, nos termos previstos no Código de Ética e Conduta da «Recuperar Portugal», ter identificado as seguintes situações de não conformidade e/ou potencial fraude:

Identificação de situação de não conformidade:
Identificação de situação de potencial fraude:

Lisboa, …… de …… 20…

Assinatura

ANEXO G – PLANO DE PREVENÇÃO DE RISCOS E CORRUPÇÃO E INFRAÇÕES CONEXAS

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

GNS
Gabinete Nacional de Segurança
PORTUGAL

O Regime Geral de Prevenção da Corrupção (RGPC), aprovado pelo Decreto-Lei n.º 109-E/2021, de 9 de dezembro, determina que todas pessoas coletivas com sede em Portugal que empreguem 50 ou mais trabalhadores devem implementar medidas de prevenção da corrupção, e dispor dos seguintes instrumentos de prevenção da corrupção: Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPRCIC); Código de conduta; Canais de denúncia; e Plano de formação e comunicação;

Além dos instrumentos previstos no diploma acima identificado, o GNS, enquanto entidade gestora de vários projetos previstos no Plano de Recuperação e Resiliência (PRR), está ainda obrigado a definir uma Declaração de Política Antifraude.

Através da elaboração dos PPRCIC pretende-se identificar as situações potenciadoras de riscos de corrupção e/ou de infrações conexas, elencar medidas preventivas e corretivas que minimizem a probabilidade de ocorrência do risco e definir a metodologia de adoção e monitorização das medidas propostas, identificando os respetivos responsáveis.

Neste sentido, e através deste instrumento de planeamento e prevenção, o GNS pretende identificar as situações potenciadoras de riscos, incluindo os de fraude, de corrupção e de infrações conexas, elencar os controlos que minimizam a sua probabilidade de ocorrência e impacto e definir o plano de ação que agregue todas as medidas de prevenção previstas, bem como os respetivos responsáveis pela sua aplicação. Define-se, ainda, os mecanismos de monitorização e revisão periódica do processo de gestão do risco, consubstanciando, desta forma, um instrumento de gestão fundamental e de grande utilidade na resposta aos desafios colocados ao GNS decorrentes da sua missão e atribuições, e no exercício das suas competências de forma ética e legal.

Na elaboração do PPRCIC do GNS foram tidas em consideração as recomendações do Conselho de Prevenção da Corrupção (CPC) e, para identificação de mecanismos de prevenção de riscos na contratação pública, a campanha “Combate ao Conluio na Contratação Pública” promovida pela Autoridade da Concorrência.

PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

Versão	Data de Reporte	Data de Aprovação	Descrição
N.º 1	26/05/2022	26/05/2022	Versão inicial
N.º 2	26/07/2023	04/10/2023	Revisão em contexto PRR

Gabinete Nacional de Segurança
Rua da Junqueira, 69 1300-342 Lisboa
Telefone: 21 040 36 00
Fax: 21 040 36 98
E-mail: geral@gns.gov.pt

ÍNDICE

CAPÍTULO 1 – ENQUADRAMENTO E ÂMBITO DE APLICAÇÃO DO PLANO DE PREVENÇÃO DE RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS

O Regime Geral de Prevenção da Corrupção, aprovado pelo Decreto-Lei n.º 109-E/2021, de 9 de dezembro, determina que todas pessoas coletivas com sede em Portugal que empreguem 50 ou mais trabalhadores devem implementar medidas de prevenção da corrupção, e dispor, de entre outros instrumentos de prevenção da corrupção, de um Plano de Prevenção de Riscos de Corrupção e Infrações Conexas (PPRCIC), vindo reforçar a Recomendação n.º 1/2009, de 1 julho, do Conselho de Prevenção da Corrupção (CPC) na qual se determina que os órgãos dirigentes máximos de entidades gestoras de dinheiros, valores ou patrimónios públicos, seja qual for a sua natureza, devem elaborar planos de gestão de risco de corrupção e infrações conexas.

Esta mesma recomendação determina, ainda, que o PPRCIC deve contemplar:

• Identificação dos riscos de corrupção e infrações conexas relativos a cada área;

• Identificação das medidas adotadas para prevenção dos riscos;

• Identificação dos responsáveis que gerem o plano de gestão de riscos;

• Elaboração de um relatório de execução anual;

• Que o PPRCIC e os relatórios de execução anuais devem ser remetidos ao CPC, bem como aos órgãos de superintendência, tutela e controlo.

O presente PPRCIC pretende ser um instrumento que permita ao GNS responder a este propósito através da adoção de mecanismos que simultaneamente garantam:

• A promoção de uma cultura de clareza e transparência no relacionamento com as entidades públicas e privadas e com os cidadãos;

• A promoção entre os seus funcionários e colaboradores de uma cultura de serviço público e de estrito cumprimento dos deveres funcionais, nomeadamente dos deveres de zelo, isenção, responsabilidade, honestidade e correção;

• O aperfeiçoamento e reforço dos mecanismos internos de controlo e supervisão;

• A definição clara das competências e responsabilidades individuais.

O PPRCIC aplica-se a todos os funcionários públicos e militares do GNS/CNCS aos demais colaboradores que, independentemente do vínculo jurídico-funcional, lhe pre-

stem trabalho ou serviços. Abrange, ainda, todas as entidades públicas e privadas e outros interessados que, diretamente ou indiretamente, venham a relacionar-se com o GNS/CNCS, devendo, neste contexto, promover-se a divulgação dos princípios vertidos neste documento por esta comunidade.

CAPÍTULO 2 - CARACTERIZAÇÃO DO GABINETE NACIONAL DE SEGURANÇA

O Gabinete Nacional de Segurança é um serviço central da administração direta do Estado, dotado de autonomia administrativa, na dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar.

A sua MISSÃO, nos termos do n.º 1 do artigo 2.º do Decreto-Lei n.º 3/2012 de 16 de Janeiro, na republicado pelo Decreto-Lei n.º 136/2017, de 6 de novembro, é "(…) garantir a segurança da informação classificada 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 informação classificada, 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.".

O Centro Nacional de Cibersegurança (CNCS) funciona no âmbito do GNS, tendo como missão "(…) contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais".

No âmbito da sua missão, as principais atividades desenvolvidas pelo GNS são a credenciação de: (i) segurança de pessoas singulares ou coletivas para administração de informação classificada; (ii) entidades de certificação eletrónica do Estado; (iii) segurança a entidades para o exercício de atividades industriais, tecnológicas e de investigação; (iv) segurança nacional às empresas de comércio e indústria de bens e tecnologias militares, de certificação de segurança a produtos e sistemas de comunicações,

de informática e de tecnologias de informação classificada, certificação das entidades gestoras de plataformas eletrónicas de contratação pública e supervisão da implementação do regulamento 910/2014 da UE.

Relativamente ao CNCS, no âmbito da sua missão, as principais atividades centram-se no desenvolvimento das capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de Cibersegurança e ciberataques, no processo de regulamentação da Lei 46/2018 de 13 de agosto que transpõe a Diretiva de Segurança das Redes da Informação (Diretiva SRI) para a legislação nacional, e na coordenação do plano de ação da ENSC 2019-2023. Com a publicação do DL 65/2021 de 30 de julho, que Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da Cibersegurança, o CNCS reforçou as suas competências enquanto Autoridade Nacional de Certificação de Cibersegurança.

A VISÃO do GNS/CNCS traduz-se em contribuir, no âmbito das suas atribuições, para um Portugal mais seguro, através de um comportamento resiliente e de um pensamento inovador.

2.1 CONJUNTO DE VALORES

Na prossecução das suas atribuições e no exercício das suas competências, a conduta do GNS/CNCS, dos seus dirigentes, trabalhadores e colaboradores civis e militares, encontra-se vinculada ao estrito respeito pelos princípios éticos gerais consagrados na lei, nomeadamente na Constituição da República Portuguesa, no Código do procedimento Administrativo, na Lei Geral do Trabalho e do Trabalho em Funções Públicas, assim como aos princípios ínsitos na Carta de Ética da Administração Pública, e nas Bases Gerais da Condição Militar, no Estatuto dos Militares das Forças Armadas, e no Regulamento de Disciplina Militar.

Em particular, o GNS/CNCS rege-se por um conjunto de valores vertidos no seu Código de Ética, como sejam:

• Lealdade, professada na prática da verdade, da fidelidade aos princípios éticos, e da constância e firmeza no compromisso assumido para com as chefias, para consigo mesmo e para com os seus pares;

• Confiabilidade, enquanto capacidade de dar resposta às solicitações externas nos

prazos determinados, mesmo em circunstâncias adversas e inesperadas;

• Honestidade, a virtude que exige coerência e sinceridade no agir, sentir e falar;

• Rigor, no fazer com seriedade de princípios, exatidão, precisão, concisão e pontualidade;

• Honra, percecionada na conduta virtuosa, na firmeza e na dignidade de carácter e que se reflete no reconhecimento público que se obtém pelo cumprimento do dever, donde resulta reputação e prestígio;

• Integridade, na assunção de responsabilidades, materializada na transparência, honestidade e equidade das decisões e atos.

No contexto de aplicação individual, organizacional, social e ambiental, o GNS/CNCS incentiva todos os seus trabalhadores e colaboradores a adotarem um comportamento assente na excelência, inovação, compromisso, e na ecologia, o que se traduz numa postura de flexibilidade e disposição para a mudança, espírito de equipa e atitude positiva e de franca cooperação, orientação para os resultados e qualidade do serviço, proatividade, responsabilidade e compromisso com o serviço, e sentido de serviço público.

O modelo de liderança adotado pelo GNS está focado nas pessoas e é praticado numa lógica inclusiva no sentido do processo de decisão não ser solitário, envolvendo os diferentes atores no processo decisório garantindo assim uma maior adesão à decisão tomada.

O GNS prossegue a sua missão e exerce as suas competências, suportado nos seguintes

instrumentos de gestão:

• Plano e Relatório de Atividades e Contas;

• QUAR;

• Balanço social;

• Orçamento e Mapa de Pessoal;

• Plano estratégico;

• Normas procedimentais e de controlo interno.

2.2 RECURSOS HUMANOS

O Mapa de Pessoal constitui um instrumento fundamental de planeamento e gestão estratégica

de recursos humanos, permitindo uma visão integrada e dinâmica desses mesmos recursos,

contribuindo para uma cultura organizacional orientada para o serviço público de acordo com

critérios de racionalização, transversalidade, eficiência e economia de custos.

O mapa de pessoal da GNS aprovado para o ano 2023 prevê 122 trabalhadores, conjugando

trabalhadores com contrato de trabalho em funções públicas, em Comissão de Serviço e Pessoal Militar e das Forças de Segurança, em função das atribuições prosseguidas e sem prejuízo das atividades transversais e comuns a todo o modelo organizacional, numa lógica de eficiência, qualidade e racionalidade.

2.3 ESTRUTURA ORGÂNICA E FUNCIONAL

De acordo o disposto no artigo 4.º do Decreto-Lei n.º 170/2007, de 3 de maio, e do artigo 5.º 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.

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. A 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.

CAPÍTULO 3 - CORRUPÇÃO E INFRAÇÕES CONEXAS

O crime de corrupção está previsto no Capítulo IV do Título V do Código Penal (CP), juntamente com outros crimes cometidos no exercício de funções públicas.

O nº 1 do artigo 372º do CP relativo ao crime de recebimento indevido de vantagem estabelece que "O funcionário que, no exercício das suas funções ou por causa delas, por si, ou por interposta pessoa, com o seu consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, que não lhe seja devida é punido com pena de prisão até cinco anos ou com pena de multa até 600 dias." O nº 2 da citada disposição estabelece que "quem por si ou por interposta pessoa, com o seu consentimento ou ratificação, der ou prometer a funcionário, ou a terceiro por indicação ou conhecimento daquele, vantagem patrimonial ou não patrimonial, que não lhe seja devida, no exercício das suas funções ou por causa delas, é punido com pena de prisão até três anos ou com pena de multa até 600 dias."

Significa o supra referenciado que os trabalhadores em funções públicas estão liminarmente impedidos de receber qualquer vantagem que não lhes seja devida, visando ou não a prática de um determinado ato. Trata-se da incriminação da simples aceitação ou solicitação de um qualquer benefício ainda que, no contexto concreto, não esteja envolvida, como contrapartida, uma ação ou omissão, contrárias ou não aos deveres do cargo.

Com esta incriminação visa o legislador evitar o risco de que a vantagem implique, ainda que futuramente, uma flexibilização da conduta do funcionário com claro prejuízo para os princípios da transparência, da justiça e da boa administração.

A corrupção propriamente dita está prevista no artigo 373º na forma passiva e no artigo 374º na forma ativa, ambos do Código Penal (CP). Na forma passiva pune-se, com pena de um a oito anos, aquele que, por si ou por interposta pessoa, com o seu

consentimento ou ratificação, solicitar ou aceitar, para si ou para terceiro, vantagem patrimonial ou não patrimonial, ou a sua promessa, para a prática de um qualquer ato ou omissão contrários aos deveres do cargo, ainda que anteriores àquela solicitação ou aceitação. Na forma ativa pune-se, por oposição, aquele que corrompe.

De acordo com o nº 1 do artigo 374º do CP, quem, por si ou por interposta pessoa, com o seu conhecimento ou ratificação, der ou prometer a funcionário, ou a terceiro por indicação ou com conhecimento daquele, vantagem patrimonial ou não patrimonial, para a prática de um qualquer ato ou omissão contrários aos deveres do cargo, ainda que anteriores àquela solicitação ou aceitação, é punido com pena de prisão de um a cinco anos".

Se o ato ou omissão não forem contrários aos deveres do cargo o infrator é punido com pena de prisão até três anos ou com pena de multa até 360 dias.

No contexto da corrupção e criminalidade conexa, há que referir explicitamente o crime de participação económica em negócio previsto no artigo 377º do CP que determina que: no seu n.º 1 "O funcionário que, com intenção de obter, para si ou para terceiro, participação económica ilícita, lesar em negócio jurídico os interesses patrimoniais que, no todo ou em parte, lhe cumpre, em razão da sua função, administrar, fiscalizar, defender ou realizar, é punido com pena de prisão até 5 anos; no seu n.º 2- "O funcionário que, por qualquer forma, receber, para si ou para terceiro, vantagem patrimonial por efeito de ato jurídico-civil relativo a interesses de que tinha, por força das suas funções, no momento do ato, total ou parcialmente, a disposição, administração ou fiscalização, ainda que sem os lesar, é punido com pena de prisão até 6 meses ou com pena de multa até 60 dias". A pena prevista no número dois é também aplicável ao funcionário que receber, para si ou para terceiro, por qualquer forma, vantagem patrimonial por efeito de cobrança, arrecadação, liquidação ou pagamento que, por força das suas funções, total ou parcialmente, esteja encarregado de ordenar ou fazer, posto que não se verifique prejuízo para a Fazenda Publica ou para os interesses que lhe estão confiados."

Importa ainda considerar, neste contexto, outros crimes previstos no CP, como: o tráfico de influências (artigo 335º), o descaminho ou destruição de objetos colocados sob o poder público (artigo 355º), o favorecimento pessoal praticado por funcionário (artigo 368º) o peculato e peculato de uso (artigos 375º e 376º), a concussão (artigo 379º), o abuso de poder (artigo 382º), e a violação de dever de segredo (artigo 383º).

Todos os crimes identificados têm em comum o facto de poderem ser ou de serem exclusivamente praticados no exercício de funções públicas.

Extrai-se das disposições penais mencionadas que o dirigente ou trabalhador em funções públicas está impedido, salvo conduta socialmente adequada e conforme usos e costumes, de receber ou solicitar qualquer vantagem ou promessa desta, seja para si ou para terceiro, seja por si ou através de interposta pessoa. Trata-se de um conjunto de normas que visam não só reprimir condutas, mas também prevenir, através dessa repressão, a concretização de um mal maior.

Ligadas ou próximas da corrupção existem outras situações igualmente prejudiciais ao bom funcionamento do Estado, suas instituições e mercados, tipificados como crimes. Em termos sucintos, poderão constituir corrupção ou infração conexa as seguintes situações:

• Desvio de recursos públicos para outras finalidades;

• Ofertas de dinheiro ou qualquer bem material para agilizar processos;

• Aceitação de gratificações ou comissões para escolher uma empresa que prestará serviços ou venderá produtos ao GNS;

• Receber e/ou solicitar dinheiro de empresas privadas para aprovar ou executar propostas/projetos que as beneficiem;

• Contratar empresas de familiares;

• Utilização de dinheiro e recursos públicos para interesse particular.

Concorrem para estas tipologias de crime vários fatores potenciam situações de corrupção ou outras infrações conexas, tais como:

• O ambiente propício;

• Qualidade da gestão e idoneidade dos gestores e decisores;

• A adequação do sistema de controlo interno;

• A ética e conduta das instituições e dos trabalhadores;

• Motivação dos trabalhadores;

• A legislação e normas de conduta.

3.1 CONFLITO DE INTERESSES

Quanto ao conflito de interesses no setor publico, este pode ser definido como qualquer situação em que um agente público, por força do exercício das suas funções, ou por causa delas, tenha de tomar decisões ou tenha contacto com 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 sabre a isenção e o rigor que são devidos ao exercício de funções públicas.

Podem igualmente ser geradoras de conflito de interesses situações que envolvam trabalhadores que deixaram o cargo público para assumirem funções privadas, como trabalhadores, consultores ou outras, porque participaram, direta ou indiretamente, em decisões que envolveram a entidade privada na qual ingressaram, ou tiveram acesso a informação privilegiada com interesse para essa entidade privada ou, também, porque podem ainda ter influência na entidade pública onde exerceram funções, através de ex-colaboradores.

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 na 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 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 inex-

istência 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 (Anexo II − Declaração de Conflito de Interesses).

CAPÍTULO 4 – RISCO

Considerando o quadro legal, bem como as normas éticas a que os funcionários públicos e militares estão vinculados e tendo presente as atribuições do GNS/CNCS, identificaram-se as áreas consideradas mais suscetíveis de geração de riscos e procedeu-se a uma classificação de acordo com a Norma da Gestão de Riscos da FERMA (Federation of European Risk Management Associations), com o documento Enterprise Risk Management – an Integrated Framework, do COSO (Committee of Sponsoring Organizatios) e com o guião disponibilizado na página web do CPC. Os riscos, após identificados e caracterizados por unidade orgânica, devem ser classificados em função do grau de probabilidade de ocorrência e da gravidade da consequência, de acordo com uma escala.

A efetiva gestão do risco pressupõe a identificação do risco, a sua comunicação, aceitação, qualificação e o estabelecimento de um plano e processo adequados para esse efeito.

4.1 CONCEITOS

Importa clarificar conceitos, em especial o conceito de “risco” e de “gestão do risco”:

• RISCO é definido como o evento, situação ou circunstância futura com a probabilidade de ocorrência e potencial consequência positiva ou negativa na consecução dos

objetivos de uma unidade organizacional". [in Plano de Prevenção de riscos de Gestão da Direção-Geral do Tribunal de Contas, pág. 8];

• GESTÃO DO RISCO é o processo através do qual as organizações analisam metodicamente os riscos inerentes às respetivas atividades, com o objetivo de atingirem uma vantagem sustentada em cada atividade individual e no conjunto de todas as atividades." [Norma de gestão de riscos, FERMA].

Tal como referido na Norma de Gestão de Riscos da FERMA, a gestão do risco não é apenas um exclusivo das entidades públicas, mas também de empresas, aplicando-se, nessa medida, a qualquer atividade ou projeto de curto ou longo prazo. A efetiva gestão do risco pressupõe a identificação do risco, a sua comunicação, aceitação, qualificação e o estabelecimento de um plano e processo adequados para esse efeito.

4.2 QUALIFICAÇÃO DO RISCO

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:

A. Probabilidade de ocorrência das situações que comportam "risco";

B. Impacto estimado das infrações.

Da conjugação destas variáveis apresenta-se a seguinte tabela, com os graus de risco que serão adotados no presente Plano, sendo que se aplicará a fórmula seguinte: Risco = Probabilidade X Impacto, onde >= 6 - Elevado; >= 4 e < 6 – Moderado, e < 4 – Fraco.

TABELA 1: QUALIFICAÇÃO DO RISCO

Tabela de Risco		Probabilidade de Ocorrência		
		Elevada	Moderada	Fraca
Impacto da Ocorrência	Elevado	Elevado	Elevado	Moderado
	Moderado	Elevado	Moderado	Fraco
	Fraco	Moderado	Fraco	Fraco

A determinação do grau (elevado, moderado ou fraco), de cada uma das variáveis que integram a definição de risco, é efetuada de acordo com:

TABELA 2: CRITÉRIOS DE GRADUAÇÃO

Impacto Ocorrência		
Elevado	Moderado	Fraco
Prejuízos significativos para o Estado Português ou para os interesses financeiros da União Europeia e a violação grave dos princípios associados ao interesse público, lesando a credibilidade do GNS/CNCS e do próprio Estado Português e da União Europeia	Prejuízos reputacionais, operacionais, financeiros, e/ou regulatórios para o Estado Português ou para os interesses financeiros da União Europeia 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 Europeia, não sendo as infrações causadoras de danos relevantes na imagem e operacionalidade do GNS/CNCS

TABELA 3: QUALIFICAÇÃO DA PROBABILIDADE

Probabilidade da ocorrência		
Elevado	Moderado	Fraco
O risco decorre de um processo corrente e frequente do GNS	O risco está associado a um processo esporádico do GNS que se admite venha a ocorrer ao longo do ano.	O risco decorre de um processo que apenas ocorrerá em circunstâncias excecionais.

4.3 ÁREAS SUSCETÍVEIS DE RISCO E MEDIDAS PREVENTIVAS DOS RISCOS

Áreas de risco identificadas:

- Apoio à Decisão
- Gestão de Projetos
- Relações Institucionais
- Contratação Pública
- Gestão Patrimonial
- Gestão de Pessoas
- Sistema de Controlo Interno
- Supervisão
- Inspeção, Fiscalização e Auditoria
- Gestão da Informação
- Emissão de credenciações, certificações e acreditações

No sentido de desenvolver medidas preventivas dos riscos de corrupção e infrações conexas, importa atentar no modelo explicativo da corrupção que identifica três fatores como uma constante dos casos conhecidos: a oportunidade, a racionalização e a pressão.

A oportunidade para a prática de ato fraudulento faz parte de uma dimensão organizacional e trata-se da que está mais facilmente ao alcance da intervenção dos serviços no sentido de diminuir as fragilidades.

A racionalização consiste na adequação mental dos indivíduos, no sentido de racionalizar a sua própria conduta, de forma a ajustar a conceção de si mesmos de tal forma que o ato praticado não lhes pareça tão condenável. Esta racionalização já faz parte de uma dimensão pessoal, de difícil intervenção por parte dos serviços, a não ser pela constante consciencialização para o problema.

A pressão diz respeito ao contexto socioeconómico do indivíduo, faz parte da dimensão pessoal e não é possível aos serviços intervir neste fator.

Identificados os riscos e atentas as variáveis inerentes aos atos de corrupção e in-

frações conexas, importa pensar as ações que pretendem prevenir tais riscos. A par das medidas de prevenção identificadas no Anexo I, e da divulgação do presente Plano de Prevenção de Riscos de Corrupção e Infrações Conexas, em termos de mecanismos gerais preventivos dos Riscos de Corrupção e Infrações, o GNS privilegia a materialização dos seguintes mecanismos:

• Acompanhamento e supervisão adequados por parte da Direção, dos Chefes de Equipa Multidisciplinares e dos Consultores-Coordenadores;

• Utilização de sistema de gestão e controlo documental através de software adequado;

• Primazia à multiplicidade de concorrentes em procedimentos de aquisição de bens e serviços, ou Empreitadas de Obras Públicas, dando prioridade ao recurso a Concursos Públicos em detrimento da adoção de Consultas Prévias e Ajustes Diretos;

• Controlo orgânico, que decorre da segregação de funções entre as diversas áreas funcionais com intervenção nos procedimentos;

• Promoção de ações internas de sensibilização para as consequências da corrupção e infrações conexas, de divulgação de manuais de procedimento e do Código de Ética e Conduta;

• Aprovação de Planos Anuais de Compras.

CAPÍTULO 5 – IDENTIFICAÇÃO DOS RESPONSÁVEIS QUE GEREM O PLANO DE GESTÃO DE RISCOS

A Equipa designada para o efeito, deve assegurar a adequada implementação do presente PPRCIC, incentivando o comportamento ético, definindo, nos respetivos níveis hierárquicos, os princípios e regras de conduta para o resto da organização e garantindo a execução de controlos internos adequados. Concomitantemente, assume-se como responsável pela execução e monitorização das medidas preventivas dos Riscos de Corrupção e Infrações Conexas, mormente, através da implementação das medidas constantes neste PPRCIC, bem como o seu restabelecimento através de normativos concorrentes, tais como Normas de Execução Permanente.

Em termos institucionais, toda a cadeia de direção e comando é responsável pela prevenção e deteção de erros e/ou irregularidades que possam estar relacionadas com atos de corrupção e de infrações conexas. Em primeira instância, a responsabilidade

é do Diretor-Geral do GNS, do Subdiretor Geral do GNS e do Coordenador do CNCS, das Chefias das Equipas Multidisciplinares e dos Consultores-Coordenadores, mas em última instância cabe a todos, através da implementação e do funcionamento contínuo de sistemas de controlo interno adequados para eliminar e/ou reduzir os erros e as fraudes.

A responsabilidade pela prevenção e deteção de fraudes, irregularidades, erros e corrupção, cabe a todos os funcionários civis e militares (dever de zelo), e colaboradores do GNS/CNCS.

Na sua conduta, procedem de acordo com critérios de razoabilidade e prudência, e devem informar o seu superior hierárquico, ou, em função da natureza da matéria envolvida, outras entidades competentes, designadamente o Ministério Público, o Tribunal de Contas, a Inspeção-geral de Finanças - Autoridade de Auditoria, o Organismo Europeu de Luta Antifraude (OLAF) ou a Procuradoria Europeia, no respeito pelas respetivas atribuições, sempre que tomem conhecimento ou tiverem suspeitas fundadas da ocorrência de atividades de corrupção, ativa ou passiva, criminalidade económica e financeira, branqueamento de capitais, tráfico de influências, apropriação ilegítima de bens públicos, de administração danosa, peculato, participação económica em negócios, abuso de poder ou violação do dever de segredo, aquisição de imóveis ou valores mobiliários em consequência da obtenção ou utilização ilícitas de informação privilegiada no exercício de funções na Administração Pública, dando especial atenção a qualquer forma de pagamentos, favores e cumplicidades que possam induzir a criação de vantagens ilícitas, de acordo com o modelo constante no Código de Conduta do GNS (Anexo III – Comunicação de situação específica de não conformidade ou potencial fraude), utilizando para tal o canal de denúncia estabelecido na entidade.

A eventual omissão do dever de denúncia ou participação pode gerar responsabilidade disciplinar e/ou penal.

O colaborador do GNS/CNCS que comunicar ou impedir a realização de atividades ilícitas, não poderá ser, por esse facto, prejudicado a qualquer título.

Entende-se por irregularidade, a violação, intencional ou não, de uma lei ou de uma norma ou princípio contabilístico ou administrativo aplicável, o que faz com que grande

parte dos erros possa, também, ser qualificada como irregularidade. Está-se geralmente perante uma fraude quando existe manipulação da lei, falsificação, alteração ou omissão voluntária de registos e/ou documento de apoio, com a intenção de obter uma representação incorreta da informação financeira ou uma apropriação ilícita de ativos ou desvio de fundos para fins diferentes daqueles para que foram atribuídos.

CAPÍTULO 6 - AÇÕES DE AFERIÇÃO DA EFETIVIDADE, UTILIDADE E EFICÁCIA DAS MEDIDAS PROPOSTAS

Com o objetivo de se aferir da efetividade, utilidade e eficácia das medidas propostas, a Direção do GNS/CNCS compromete-se a:

• Criar métodos e definir procedimentos para implementação das medidas preventivas previstas no Anexo I do presente Plano de Prevenção de Riscos de Corrupção e Infrações Conexas;

• Criar uma Equipa de acompanhamento do Plano de Prevenção de Riscos de Corrupção e Infrações Conexas;

• Divulgar junto dos funcionários civis e militares, e colaboradores do GNS/CNCS os relatórios decorrentes dos controlos internos ou externos, relativos ao cumprimento das normas de procedimentos vigentes, por parte dos funcionários;

• Garantir que as medidas de mitigação e as ações de controlo interno são do conhecimento geral, dos militares e civis do GNS/CNCS através da fomentação de ações de divulgação e esclarecimento com vista ao fortalecimento de uma cultura ética anticorrupção;

• No final de cada ano, a Equipa de acompanhamento elaborará um relatório de execução do Plano, o qual deve contemplar:

- O balanço das medidas adotadas e das medidas por adotar com identifi cação dos fatores que impediram a sua concretização;

- A identificação dos riscos que foram reduzidos e dos riscos que se mantêm;

- A eventual identificação dos riscos não contemplados no Plano;

- A eventual necessidade de se proceder à revisão do Plano;

- O Semestralmente a Equipa deve informar a direção do GNS/CNCS de quaisquer condição observadas que possam suscitar situações enquadráveis no espirito deste documento.

CAPÍTULO 7 - ANEXO A - IDENTIFICAÇÃO DOS RISCOS DE CORRUPÇÃO E INFRAÇÕES CONEXAS E MEDIDAS PREVENTIVAS E CORRETIVAS (RESERVADO)

GABINETE NACIONAL DESEGURANÇA
CENTRO NACIONAL DE CIBERSEGURANÇA

Rua da Junqueira, 69
1300-342 Lisboa
PORTUGAL
+351 210 497 400
www.gns.gov.pt / geral@gns.gov.pt
www.cncs.gov.pt / cncs@cncs.gov.pt