GABINETE NACIONAL DE SEGURANÇA
E
CENTRO NACIONAL DE CIBERSEGURANÇA

Plano de Atividades

2025

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

PÁGINA DEIXADA EM BRANCO

ÍNDICE

SUMÁRIO EXECUTIVO

As atividades do GNS/CNCS estão alinhadas com os objetivos para o desenvolvimento sustentável (ODS), em consonância com o compromisso assumido por Portugal relativamente à implementação da Agenda 2030, e em sintonia com o que se encontra previsto na proposta de Lei de Orçamento de 2025.

O planeamento a desenvolver em 2025 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, destacando-se a necessidade da execução das medidas e marcos/metas do investimento TD C19 i03 do PRR em harmonia com os objetivos vertidos no programa do XXIV Governo Constitucional.

O GNS/CNCS dará continuidade à concretização do seu plano estratégico, através duma atuação resiliente e sustentável, 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, valores e 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 2025, 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 adaptação 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 2025, um quantitativo global de 159 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 € 8.099.032 dos quais € 5.245.801 são respeitantes à atividade do CNCS. No âmbito do Plano de Recuperação e Resiliência está previsto um investimento de € 34.352.843. Com a Lei do OE-2025 e o subsequente decreto-lei de execução orçamental poderá contemplar cativações 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 2025.

Em conclusão, para o ano de 2025, 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 às mudanças organizacionais bem como 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 qualificar os recursos humanos e adequar as infraestruturas para os acomodar, recorrendo às medidas previstas no PRR;
- **Estrutural –** em que se pretende otimizar os processos de gestão de recursos humanos, processos de contratação pública e ainda no sistema de gestão e controlo 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 2025, o GNS/CNCS pretende dar continuidade e concluir um conjunto de ações, de grande visibilidade externa dando sequência à implementação do novo Regime Jurídico de Cibersegurança que transpõe a Diretiva NIS2, incluindo o reforço dos mecanismos de regulação e supervisão. Igualmente será prosseguida a 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 (C-HUB); 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 de Resposta a Incidentes (CERT.PT) com os instrumentos e as ferramentas necessárias para incrementar a sua capacidade de operar e interagir com a comunidade e autoridades públicas de Cibersegurança.

ESTRATÉGIA E OBJETIVOS

O Plano de Atividades, constitui-se como um referencial de gestão e administração do GNS e do CNCS para o ano de 2025, tendo em conta as respetivas natureza, missão e atribuições.

Os objetivos estratégicos 1, 2 e 3 pressupõem o desígnio de um novo ciclo de orientação estratégica sendo o OE4 uma continuidade reforçada na qualidade e melhoria contínua dos Recursos Humanos. As suas linhas de ação visam prosseguir com a edificação equilibrada de capacidades, incluindo a respetiva sustentação, continuar 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, com a transmissão da estratégia a todos os Departamentos e recolhendo destes os contributos para 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.

QUAR

Para 2025, são estabelecidos 4 Objetivos Estratégicos para constarem no QUAR, representativos das ambições macro da organização.

OE1: Planear a execução do novo modelo institucional da Cibersegurança.
OE2: Rever o regime jurídico da informação classificada.
OE3: Assegurar a capacidade criptográfica nacional.
OE4: Reforçar a formação e bem-estar das pessoas trabalhadoras.

Destes objetivos estratégicos, irão derivar os respetivos objetivos operacionais, inscritos no QUAR-2025, cuja concretização será obtida mediante a realização das atividades de cada uma das unidades orgânicas. Abaixo, apresenta-se um esquema QUAR GNS/CNCS para melhor perceção da inter-relação entre os objetivos estratégicos, operacionais e respetivos indicadores mais representativos da atividade desenvolvida e que melhor refletem as linhas estratégicas definidas.

Assim, o OE1 estabelece a vontade de se proceder à reestruturação deste organismo derivado da transposição da NIS2. Para isso, foram identificados dois objetivos operacionais, OP1 e OP2, em que um visa elaborar uma proposta de regulamentação que faça o enquadramento desta reorganização, OP1, cujo indicador 1 se pode visualizar, medindo percentualmente o trabalho desenvolvido face ao tempo estipulado. Assim, pretende-se que o documento se desenvolva a um ritmo de aproximadamente 15% por mês tendo como meta 31 de julho e o OP2 que identifica o desenvolvimento de uma plataforma de autoidentificação e qualificação das entidades cuja execução se prevê igualmente, monitorizar e concretizar, a um ritmo de 15% por mês, havendo a ambição de ter a plataforma em funcionamento até 31 de julho de 2025, indicador 2. A monitorização deste OE é feita pelo Núcleo de Apoio ao Coordenador (NAC) tendo sido estipulado que a meta deste OE seria de 100%.

O OE2 visa desenvolver os projetos legislativos e os estudos e ações de suporte tendentes à revisão do regime jurídico da informação classificada, incluindo a substituição dos SEGNAC (normas e instruções de Segurança Nacional), com recurso à aquisição de serviços para o efeito, para o cumprimento desta ambição (OP3). O indicador 3, "Percentagem da execução das tarefas com vista à obtenção de projetos legislativos e dos estudos e ações de suporte tendentes à revisão do regime jurídico da informação classificada", permitirá monitorizar a execução deste objetivo através da realização de tarefas que constituem cada uma das 4 seguintes fases:

- 1.ª fase – Preparação das peças procedimentais e restante documentação de suporte à decisão de contratar – até 28 FEV2025, com a decisão de contratar (4 semanas) 10%

- 2.ª fase – Adjudicação da proposta – até 30 MAR2025, com a decisão de adjudicação (4 semanas) 10%

- 3.ª fase - Execução contratual 1.ª parte – Entrega dos estudos científicos e dos projetos legislativos e sua documentação de suporte – até 30 SET2025 (6 meses) 65%

- 4.ª fase – Execução contratual – Realização de workshops e entrega dos projetos legislativos e sua documentação de suporte finais – até 15DEZ2025 (2,5 meses) 15%

O OE3 pretende assegurar a adoção de uma solução criptográfica nacional, ambicionando por disponibilizar essa solução a 150 utilizadores finais, OP4. Este desiderato começa pela elaboração de um plano de industrialização que será desenvolvido pelo Departamento de Gestão da Informação Classificada e Criptografia (DGICC) cuja monitorização será feita percentualmente em três fases conforme abaixo indicado:

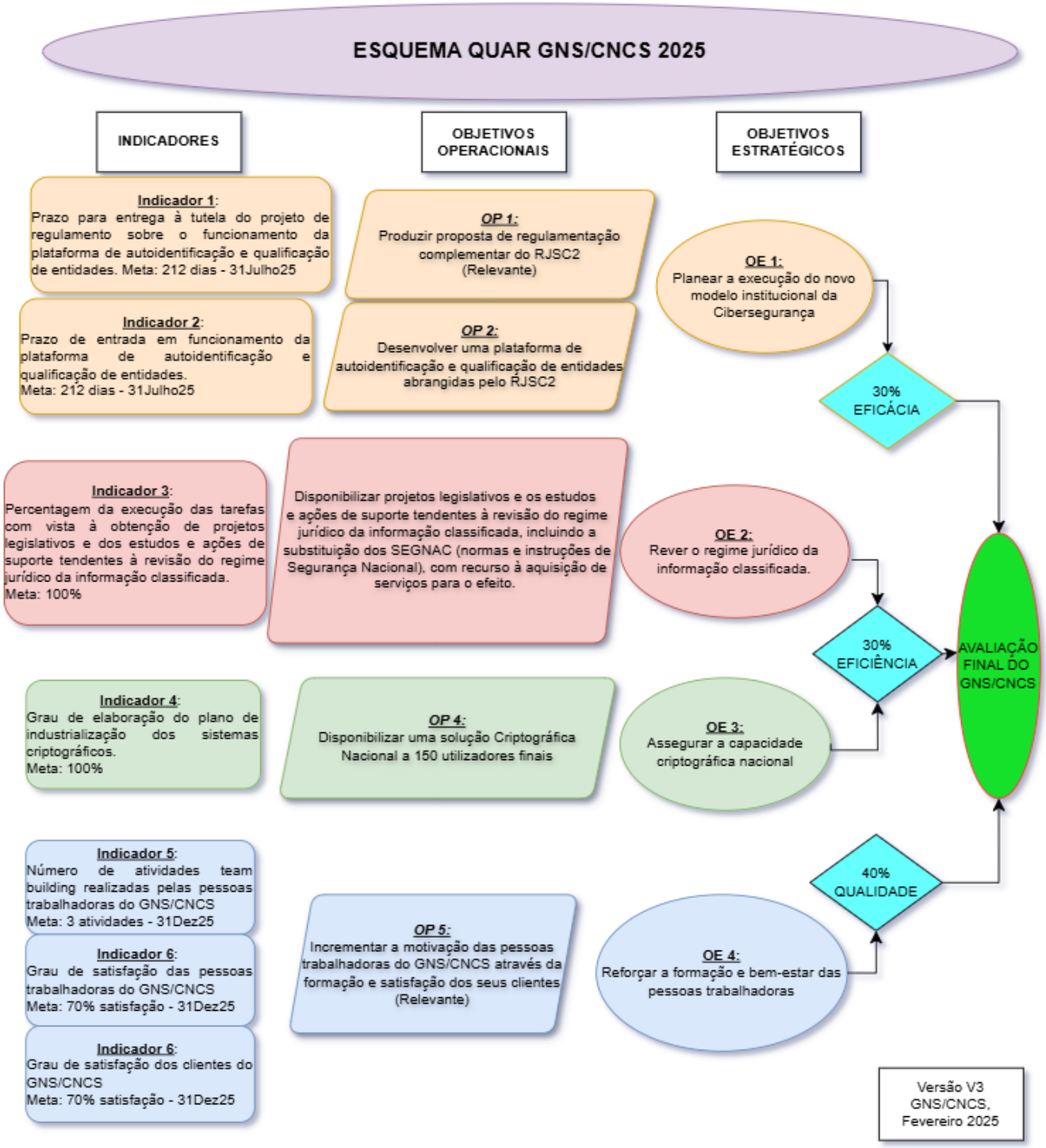
- 1.ª fase – elaboração do estudo e metodologia para o projeto de industrialização - até 31MAR2025 - 25%

- 2.ª fase – execução do projeto - até 30ABR2025 - 50%

- 3.ª fase – entrega do projeto de industrialização da máquina de cifra - até 31 MAI2025 25%

Este OE é plurianual pelo que continuará a ser acompanhado e monitorizado no ano seguinte.

Por fim, o OE4 tem como desiderato o reforço da formação e bem-estar das pessoas trabalhadoras do GNS/CNCS com o OP5 a identificar a necessidade contínua de motivar as pessoas para a obtenção de melhor qualidade de trabalho. Para isso, são criados os indicadores 5, 6 e 7 que permitem avaliar o número de atividades de *team building* realizadas e inquéritos internos de verificação de satisfação com vista à melhoria contínua (5 e 6). O indicador 7, aliado aos anteriores, visa a avaliação da satisfação dos clientes do GNS/CNCS através de inquéritos externos. Considera-se que a meta 70% do OE é atingível e desejável porque só com pessoas motivadas e em sintonia com os objetivos da organização se conseguem obter os resultados desejados com qualidade. A monitorização destes indicadores será feita pelo Núcleo de Apoio à Direção (NAD) como responsável pelos Recursos Humanos (RH).


ESQUEMA QUAR GNS/CNCS 2025
INDICADORES
OBJETIVOS OPERACIONAIS
OBJETIVOS ESTRATÉGICOS
Indicador 1:
Prazo para entrega à tutela do projeto de regulamento sobre o funcionamento da plataforma de autoidentificação e qualificação de entidades. Meta: 212 dias - 31Julho25
OP 1:
Produzir proposta de regulamentação complementar do RJSC2 (Relevante)
OE 1:
Planear a execução do novo modelo institucional da Cibersegurança
Indicador 2:
Prazo de entrada em funcionamento da plataforma de autoidentificação e qualificação de entidades.
Meta: 212 dias - 31Julho25
OP 2:
Desenvolver uma plataforma de autoidentificação e qualificação de entidades abrangidas pelo RJSC2
30% EFICÁCIA
Indicador 3:
Percentagem da execução das tarefas com vista à obtenção de projetos legislativos e dos estudos e ações de suporte tendentes à revisão do regime jurídico da informação classificada.
Meta: 100%
Disponibilizar projetos legislativos e os estudos e ações de suporte tendentes à revisão do regime jurídico da informação classificada, incluindo a substituição dos SEGNAC (normas e instruções de Segurança Nacional), com recurso à aquisição de serviços para o efeito.
OE 2:
Rever o regime jurídico da informação classificada.
30% EFICIÊNCIA
AVALIAÇÃO FINAL DO GNS/CNCS
Indicador 4:
Grau de elaboração do plano de industrialização dos sistemas criptográficos.
Meta: 100%
OP 4:
Disponibilizar uma solução Criptográfica Nacional a 150 utilizadores finais
OE 3:
Assegurar a capacidade criptográfica nacional
Indicador 5:
Número de atividades team building realizadas pelas pessoas trabalhadoras do GNS/CNCS
Meta: 3 atividades - 31Dez25
Indicador 6:
Grau de satisfação das pessoas trabalhadoras do GNS/CNCS
Meta: 70% satisfação - 31Dez25
Indicador 6:
Grau de satisfação dos clientes do GNS/CNCS
Meta: 70% satisfação - 31Dez25
OP 5:
Incrementar a motivação das pessoas trabalhadoras do GNS/CNCS através da formação e satisfação dos seus clientes (Relevante)
OE 4:
Reforçar a formação e bem-estar das pessoas trabalhadoras
40% QUALIDADE
Versão V3 GNS/CNCS, Fevereiro 2025

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)

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

Meta: 100% (31 março)

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), se necessário).

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).

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

Indicador: Número de Inspeções.

Meta 1: Subregistos / Postos de Controlo – 11 / 1.

Meta 2: Centros Criptográficos - 6.

Meta 3: Empresas – 29.

IA102- Realizar e coordenar a atividade inspetiva internacional.

Indicador: Número de Inspeções a Embaixadas e Postos Diplomáticos.

Meta: 4.

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 2025, o desenvolvimento e implementação de três formações, no formato e-learning, tendo em vista o cumprimento e conclusão do projeto financiado pelo PRR, iniciado em 2022, dando continuidade à mudança de paradigma da formação do GNS, que teve o seu início com a criação e implementação do Curso de Introdução à Segurança da Informação Classificada (CISIC).

Em simultâneo, procura-se manter os elevados índices de satisfação que têm caracterizado estas formações.

O Departamento de DF elege e destaca nas suas atividades para 2025, 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 UE, 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 projetos legislativos e os estudos e ações de suporte tendentes à revisão do regime jurídico da informação classificada, incluindo a substituição dos SEGNAC (normas e instruções de Segurança Nacional), com recurso à aquisição de serviços para o efeito.

(OP3: Objetivo operacional do QUAR 2025)

Indicador 3: Percentagem da execução das tarefas com vista à obtenção de projetos legislativos e dos estudos e ações de suporte tendentes à revisão do regime jurídico da informação classificada.

Este indicador permitirá monitorizar a execução deste objetivo através da realização de tarefas que constituem cada uma das 4 seguintes fases:

- 1.ª fase – Preparação das peças procedimentais e restante documentação de suporte à decisão de contratar – até 28 FEV2025, com a decisão de contratar (4 semanas) 10%
- 2.ª fase – Adjudicação da proposta – até 30 MAR2025, com a decisão de adjudicação (4 semanas) 10%
- 3.ª fase - Execução contratual 1.ª parte – Entrega dos estudos científicos e dos projetos legislativos e sua documentação de suporte – até 30 SET2025 (6 meses) 65%
- 4.ª fase – Execução contratual – Realização de workshops e entrega dos projetos legislativos e sua documentação de suporte finais – até 15DEZ2025 (2,5 meses) 15%

Meta: 100% a 15 de dezembro

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 – Doutrina (NATO; União Europeia; Nacional).

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

IA105 –Acordos.

Indicadores: Número de acordos em trabalho e assinatura de Acordos bilaterais.

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: 50 entidades.

Indicador 2: Processo de certificação do eSEIF.

Meta: 75% 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 – Disponibilizar uma solução Criptográfica Nacional a 150 utilizadores finais

(OP4: Objetivo operacional do QUAR 2025 - relevante).

Indicador 4: Grau de elaboração do plano de industrialização dos sistemas criptográficos.

Este indicador permitirá monitorizar a execução deste objetivo através da realização de tarefas que constituem cada uma das seguintes fases:

- 1.ª fase – elaboração do estudo e metodologia para o projeto de industrialização - até 31MAR2025 - 25%
- 2.ª fase – execução do projeto - até 30ABR2025 - 50%
- 3.ª fase – entrega do projeto de industrialização da máquina de cifra - até 31 MAI2025 25%

Este OE é plurianual pelo que continuará a ser acompanhado e monitorizado no ano seguinte.
Meta: 31 de maio

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 março de 2026

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: Finalizar a entrega dos HSMT 2.0 aos utilizadores finais.

Meta: 30 de junho

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, propor a avaliação, 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 avaliações de *zoning* de infraestruturas, bem como limpezas eletrónicas em áreas sensíveis onde seja tratada informação com necessidades especiais de segurança.

Segurança das Infraestruturas

Contribui para a Acreditação ou 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 e apoiar 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 nacional responsável pela componente codificada do Programa Espacial da União Europeia (PEUE), competindo-lhe nomeadamente efetuar a acreditação de segurança das infraestruturas afetas ao PEUE em território nacional e efetuar a 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 (alínea j) do ponto 3 do artigo 2º do Decreto-Lei n.º 136/2017, de 6 de novembro, que republica o Decreto-Lei n.º 3/2012, de 16 de janeiro). O Regulamento (UE) n.º 910/2014 foi recentemente alterado pelo Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho de 11 de abril de 2024, no que diz respeito à criação do Quadro Europeu de Identidade Digital.

Apoiam também 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; (alínea m) do ponto 3 do artigo 2º do Decreto-Lei n.º 136/2017, de 6 de novembro, que republica o Decreto-Lei n.º 3/2012, de 16 de janeiro).

A atividade do SDTI para 2025 traduz-se assim nos seguintes conjuntos de objetivos operacionais e atividades correntes:

OBJETIVOS OPERACIONAIS

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

Indicador 1: Enviar para aprovação o Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada.

Meta: 30 de março

SDTI_P108- Implementar o Laboratório TEMPEST em parceria com o Centro Laboratorial e Normalização (CLN) da ANACOM.

Indicador 1: Criar o normativo necessário para a Operacionalização do Laboratório TEMPEST.

Meta: 30 de agosto concretizado a 100%

Indicador 2: Certificação do Laboratório TEMPEST.

Meta: 30 de dezembro

SDTI_P109- Robustecer a capacidade de contramedidas eletrónicas.

Indicador 1: Prazo para manifestação de necessidades para aquisição de contramedidas eletrónicas para o domínio raio-x.

Meta: 30 de março

Indicador 2: Preparação da Norma Técnica referente à condução de avaliações no âmbito acústico.

Meta: 30 de dezembro

Indicador 3: 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_P110- Otimizar o 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: 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 abril

SDTI_P111 - Edificação do Centro de Operações do Espaço de forma a permitir a implementação da capacidade de comunicações e posicionamento satélite seguras.

Indicador 1: Apetrechamento da sala de operações com a Sina Mission Network.

Meta: 31 de março

Indicador 2: Edificação da componente Govsatcom – fase 1 (instalação da componente RUE).

Meta: 31 de março

Indicador 3: 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_P112- Implementar o primeiro segmento rede de comunicação quântica inovadora e ultrasegura nas infraestruturas de fibra ótica existentes em Portugal, ligando diferentes entidades públicas na Área Metropolitana de Lisboa (AML), no âmbito do projeto internacional *Portuguese Quantum Communications Infrastructure* (PTQCI).

Indicador: Aquisição de equipamentos para os *Datacenters* dos nós

Meta: 31 de janeiro

Indicador: Testes de Auditoria funcionais e de segurança

Meta: 30 de maio

Indicador: Desenvolvimento do Plano de Governação

Meta: 3 de setembro

SDTI_P113- Desenvolver a implementação do acesso descentralizado a cidadãos ou empresas de registos públicos do GNS no âmbito da credenciação de segurança recorrendo à framework EBSI/Blockchain. (Plurianual)

Indicador: Prova de conceito sobre modo de funcionamento.

Meta: 28 de fevereiro

Indicador: Concretização da prova de conceito.

Meta: 31 de novembro

SDTI_P114- 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) com as alterações efetuadas pelo Regulamento (UE) 2024/1183.

Indicador 1: Revisão do DL 12/2021 (novo eIDAS e alteração do SCEE).

Meta: 31 de dezembro corresponde a 100% da apresentação da proposta

Indicador 2: Elaboração de comunicação relativamente a entidades de registo (ordens profissionais, instituições bancárias…).

Meta: 30 de abril corresponde a 100% da apresentação da proposta

Indicador 3: 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: 31 de dezembro corresponde a 100% da apresentação da proposta

SDTI_P115- Desenvolvimento da Norma Técnica (NT) do GNS sobre os requisitos de Segurança Física para a proteção da Informação Classificada (IC).

Indicador 1: NT do GNS sobre os requisitos de Segurança Física para a proteção da IC.

Meta: 31 de outubro.

INDICADORES DE ATIVIDADE

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

Referência: 2

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

Referência: 6

IA117- Número de avaliações de Zoning.

Referência: 3

IA118- Número de Limpezas Eletrónicas.

Referência: 8

IA119- Número de Avaliações Acústicas.

Meta: 3

IA120 - Elaborar os diversos processos de acreditação PRS das empresas nacionais;

Referência: 3

IA121 - Inspecionar os sites nacionais da área do espaço (EGNOS Lisboa, EGNOS Madeira, SST) e elaborar os respetivos processos de acreditação;

Referência: 2

IA122 - Criação/participação de novos processos transformacionais no âmbito da eID e Serviços de Confiança.

Referência: 1

IA123 - Pedidos de esclarecimentos gerais s/ TSP, Plataformas, outras (reuniões e helpdesk).

Referência: 42

IA124 - Pareceres enquadrados (Âmbito no Regulamento eIDAS, PECP, outros).

Referência: 5

IA125 - Auditorias/inspeção TSP (Regulamento eIDAS).

Referência: 3

IA126 - Atualização da TSL (Trusted List).

Referência: 5

IA127 - Credenciação e/ou renovação da credenciação de auditores de segurança.

Referência: 2

IA128 - 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 2024.

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 2025.

OBJETIVOS OPERACIONAIS

DC_P301 – Fomentar a submissão dos processos de credenciação por via eletrónica (pessoas singulares e coletivas)

Indicador: Número total de processos solicitados

Meta: 80%

DC_P302 – Garantir a desmaterialização dos processos de credenciação em arquivo

Indicador: Número de processos desmaterializados em 2025 (Implica o cumprimento dos processos referidos nas notas abaixo)

Nota 1: Número de processos triados (prontos para desmaterialização, organizados fisicamente e expurgados de informação que comportam dados de terceiros bem como de informação redundante).

Nota 2: Número de Certificados de Destruição emitidos.

Nota 3: Número de processos Destruídos.

Meta: 15%

DC_P303 – Incrementar a cultura de segurança no âmbito da Informação Classificada

Indicador 1 - Reuniões plenárias com os encarregados de segurança das empresas credenciadas.

Meta: 2 (uma por semestre).

Indicador 2 - Reunião com Administrações de empresas (GNS/SIS)

Meta: 4 (uma por trimestre)

Indicador 3 – Reunião com Entidades de Vetting que colaboram o GNS

Meta: 1 por ano

INDICADORES DE ATIVIDADE

IA128 – Credenciações de segurança em 2025.

Indicador 1: Rácio anual.

Indicador 2: Rácio de credenciações de segurança de pessoas singulares emitidas CRESO/PAPEL.

Indicador 3: Rácio de credenciações de segurança de pessoas coletivas emitidas CRESO/PAPEL.

IA129 - Comunicação interinstitucional no âmbito da Credenciação de Segurança

Indicador 1: Número de respostas a pedidos de Vetting.

Indicador 2: Número de RfV e FSCIS processados.

Indicador 3: 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_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.

Indicador: Acompanhamento do processo de implementação

Meta: 25% a 31 de dezembro

Risco: Demora na entrega de equipamentos.

IRC_PI103- Implementação do “Disaster Recovery”.

Indicador: Alcançar a Inicial Operability Capability (IOC).

Meta: 31 de dezembro

Risco: Capacidade de resposta do EMGFA.

IRC_P118 – Implementar Cloud on Prem da Rede Corporativa

Indicador: Grau de implementação da rede

Meta: 30 de junho

IRC_P119 – Implementar infraestrutura PTQCI

Indicador: Grau de implementação da infraestrutura

Meta: 30 de junho

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 de seguida.

OBJETIVOS OPERACIONAIS

NAD_G202 – Desenvolvimento de novas funcionalidades e melhorias do sistema CRESO (CRESO+)

Indicador: Taxa de execução da implementação das novas funcionalidades.

Meta: 80%

NAD_G203 – Incrementar a motivação das pessoas trabalhadoras do GNS/CNCS através da formação e satisfação dos seus clientes.

(OP5: Objetivo operacional do QUAR 2025 – Relevante).

Indicador 5: Número de atividades de *team building* realizadas pelas pessoas trabalhadoras do GNS/CNCS.

Meta: 3.

Indicador 6: Grau de satisfação das pessoas trabalhadoras do GNS/CNCS.

Meta: 70%

Indicador 7: Grau de satisfação dos clientes do GNS/CNCS.

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 - Elaboração e disponibilização de templates de RH e Faq's

Indicador: Data da disponibilização no Portal da Intranet

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_G303 – Reforçar a Segurança Física das instalações.

Indicador 1: Modernização dos equipamentos de controlo de acesso das viaturas.

Meta: 31 de outubro.

Indicador 2: Modernização dos terminais multifator nas Áreas de Segurança de Classe 1 do GNS/CNCS e integração das novas capacidades na rede de Segurança mais recente.

Meta: 31 de outubro.

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

Meta: 31 de outubro.

NAD_G304 – Reforço do treino de Segurança.

Indicador: Realização de dois exercícios de evacuação.

Meta: 19 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.

NÚCLEO DE APOIO AO COORDENADOR (NAC)

O Núcleo de Apoio ao Coordenador (NAC) do CNCS compreende diferentes dimensões de apoio direto à tomada de decisão. Estão afetas a esta área as atividades e tarefas relacionadas com o 1) Controlo de Gestão, sendo o seu maior foco dirigido à monitorização da execução financeira e material transversal ao CNCS, com os 2) Assuntos Jurídicos transversais ao CNCS, que vão desde as necessidades dos departamentos do CNCS às questões da relação jurídica do CNCS com entidades externas, nacionais e internacionais, e ainda das 3) Relações Internacionais, também elas de componente transversal, perspetivando uma coordenação dos temas entre os diferentes Departamentos do CNCS que atuam em fora internacionais. Estão ainda afetas ao NAC atividades, tanto a nível nacional como internacional, de apoio e desenvolvimento de políticas públicas no âmbito da missão do CNCS.
O NAC é caracterizado por uma forte componente de reação, adaptação e ajustamento em atividades de apoio à tomada de decisão em virtude da relação do CNCS com i) a área governativa que o tutela, nomeadamente na resposta a solicitação de informação ou de pareceres, bem como com ii) os departamentos do CNCS e aos requisitos emergentes das atividades pelos quais são responsáveis – planeadas e não planeadas – e iii) ainda em resultado da dinâmica das agendas estratégicas e de políticas públicas nos contextos europeu e internacional em que Portugal se insere.
Assim, o presente Plano de Atividades 2025 do Núcleo de Apoio ao Coordenador identifica o conjunto de atividades e atribuições que lhe estão conferidas, destacando-se, igualmente, algumas iniciativas e atividades que se antevê ter impacto em cada área de atividades do NAC.

Controlo de Gestão (CG)

As atividades desenvolvidas para o efetivo controlo de gestão implicam uma ação diária na recolha e validação de informação relativa à execução financeira e material, e a necessária articulação não apenas com os serviços transversais do GNS – a ADMLOG e PMOs – mas também com estruturas externas para estes efeitos – por exemplo a Estrutura de Missão Recuperar Portugal para as matérias relacionadas com o Plano de Recuperação e Resiliência (PRR). Em 2025 prevê-se continuar a produção e acompanhamento dos instrumentos de gestão (orçamento, plano de atividades, relatório de atividades, plano de formação e SIADAP) e efetuar o controlo aos investimentos do CNCS previstos no PRR e demais financiamentos europeus. Espera-se que em 2025 a atividade de controlo de gestão beneficie da implementação de uma ferramenta de controlo analítico, pelo que a esta área será requerido um incremento de atividades para a definição de necessidades e implementação da ferramenta em estreita cooperação com os serviços transversais do GNS.

Assuntos Jurídicos (AJ)

Com elevada dependência de atividades de outros Departamentos do CNCS, a análise e emissão de pareceres jurídicos prevê-se maioritariamente relacionada com processos de aquisição e contratação de bens e serviços – atual e futura. É esperado, igualmente, que esta área de atividade venha a ser solicitada para respostas a solicitações relacionadas com a relação jurídica do CNCS com terceiros, nomeadamente em protocolos ou memorandos de entendimento. É nesta vertente jurídica que se enquadra a função de Secretário da Comissão de Avaliação de Segurança constituída no âmbito do Conselho Superior de Segurança do Ciberespaço, bem como o Secretariado do próprio do Conselho Superior de Segurança do Ciberespaço. Estas duas funções requerem um esforço no desenvolvimento das atividades de preparação e acompanhamento dos trabalhos, incluindo a preparação de documentação pré e pós reuniões. Ainda neste campo são desenvolvidas as atividades associados ao Secretariado da Comissão de Planeamento de Emergência da Cibersegurança. É esperado que à equipa afeta aos assuntos jurídicos seja requerido um incremento de tarefas relacionadas com a operacionalização da transposição da Diretiva (UE) 2022/2555 (Diretiva NIS 2) e ainda uma especial atenção com a transposição da Diretiva (UE) 2022/2557 (Diretiva CER), nomeadamente na produção de propostas de regulamentos e peças jurídicas relacionadas em particular durante o primeiro semestre do ano.

Relações Internacionais (RI)

As atividades associadas às gestão, coordenação e execução de Relações Internacionais continuarão, em 2025, o acompanhamento dos trabalhos em fora internacionais – como a Counter Ransomware Initiative, a OSCE, OCDE ou as relações bilaterais com congéneres – e europeus – como o Conselho da União Europeia no apoio ao Ministério dos Negócios Estrangeiros, o NIS Cooperation Group e alguns dos seus work streams, o Centro Europeu de Competências e os seus grupos de trabalho, o Grupo Informal de Autoridades de Inteligência Artificial e a relação deste com a estrutura de governação a adotar em Portugal para efeitos do Regulamento da Inteligência Artificial, perspetivando-se uma estreita relação deste também com os grupos de trabalho no âmbito do Conselho para o Digital na Administração Pública , entre outros. Nestas matérias são desenvolvidas ações de colaboração interna ao CNCS, e em alguns casos com o GNS, mas também no campo da cooperação com entidades e autoridades nacionais. Antecipando uma nova visão estratégica para União Europeia na sequência de um novo colégio de Comissários Europeus, em 2025 antecipam-se algumas iniciativas estratégicas no reforço da definição e cooperação das instituições e agências da União Europeia, bem como na sequência da entrada em vigor de importantes atos legislativos europeus como o Cyber Solidarity Act, Cyber Resilience Act e a própria transposição da Diretiva (UE) 2022/2555 (Diretiva NIS 2) com implicações ao nível das estruturas europeias.

Apoio ao Coordenador AC)

As atividades com vista ao apoio direto ao coordenador do CNCS para a tomada de decisão agregam um conjunto de ações que ultrapassam o âmbito do controlo de gestão, prevendo tarefas associadas à contratação de recursos humanos (entrevistas, documentação e relatórios, articulação com os serviços transversais do GNS), elaboração de documentos relacionados com a gestão e tomadas de posição do CNCS, agendamento e acompanhamento de reuniões, incluindo operacionais ou com entidades externas, bem como as decisões ali tomadas, entre outras.

Tendo em perspetiva da adoção do novo Regime Jurídico de Cibersegurança que transpõe a Diretiva NIS 2, antecipa-se no NAC o desenvolvimento de ações e iniciativas com vista à implementação do quadro organizacional resultante daquele diploma. Nesse sentido, e antecipando essa adaptação, procurar-se-á identificar o padrão seguido ao nível da União Europeia para as estruturas institucionais da governança da cibersegurança na sequência, também, da transposição da Diretiva NIS 2 nos diferentes Estados-Membros. Preconiza-se ainda a necessidade de proceder à coordenação do processo de implementação da infraestrutura tecnológica necessária para responder aos requisitos impostos pela Diretiva NIS 2, assim como à adaptação de aspetos organizacionais como o mapa/quadro de pessoal, o orçamento ajustado e, ainda, a proposta de nova lei orgânica.

OBJETIVOS OPERACIONAIS

NAC_PI100 – Produzir proposta de regulamentação complementar do RJSC2

(OP1: Objetivo operacional do QUAR 2025).

Indicador 1: Prazo para entrega à tutela do projeto de regulamento sobre o funcionamento da plataforma de autoidentificação e qualificação de entidades.

Meta: 31 de julho.

DEPARTAMENTO DE DESENVOLVIMENTO E INOVAÇÃO (DDI)

O Departamento de Desenvolvimento e Inovação (DDI) é responsável pela capacitação de cidadãos e profissionais em cibersegurança, promovendo a sensibilização, formação técnica avançada e o desenvolvimento de competências. Além disso, contribui para o conhecimento do panorama nacional de cibersegurança através da análise e divulgação de informação estratégica. Gere também a comunicação interna e externa do CNCS, assegurando uma comunicação eficaz e alinhada com a missão da organização, promovendo o reconhecimento da marca e reforçando a identidade visual.

As principais iniciativas do departamento incluem a sensibilização e capacitação em cibersegurança de diversos públicos, oferecendo cursos de e-learning, sessões de sensibilização e competições especializadas como as Capture The Flag (CTF). A coordenação do Consórcio do Centro Internet Segura também permite a oferta de serviços de sensibilização sobre segurança digital e apoio à população. Estes serviços incluem campanhas adaptadas a diferentes idades e perfis, além de fornecer suporte sobre questões de segurança digital. O programa C-Academy oferece formação avançada em cibersegurança para a administração pública e o setor privado, preparando os profissionais para enfrentar os desafios do ciberespaço.

O Observatório de Cibersegurança analisa o estado da cibersegurança a nível nacional, não descurando a evolução destas matérias ao nível internacional, monitoriza tendências e elabora relatórios que fornecem dados relevantes para a formulação de políticas públicas e decisões estratégicas. Estas iniciativas destacam o papel crucial do CNCS na promoção da cibersegurança em Portugal, garantindo uma comunicação eficaz e contribuindo para uma visão informada e estratégica sobre o ecossistema da cibersegurança.

Sensibilização e Capacitação (SC)

No âmbito da sensibilização, o plano de atividades para 2025 dará continuidade ao trabalho desenvolvido pelo consórcio e pelo CNCS, assegurando a manutenção das iniciativas e ações de treino já em curso. Entre as principais atividades, destaca-se a implementação do Roadshow ZigZaga da Net, direcionado a alunos do pré-escolar e 1º ciclo, e o Roadshow CIS - Cybersecurity LAB, em colaboração com a Direção-Geral da Educação (DGE). Estas iniciativas serão acompanhadas pela dinamização do Dia da Internet Mais Segura 2025, em parceria com os membros do consórcio, e pela criação de recursos digitais e interativos que reforçarão o CIS - Cybersecurity LAB. Serão ainda desenvolvidos conteúdos sobre boas práticas, com o objetivo de sensibilizar e fortalecer comportamentos de cibersegurança entre os cidadãos.
Em colaboração com o Instituto para os Comportamentos Aditivos (ICAD), será dinamizado o jogo digital "Eu e os Outros", além da participação no Grupo Informal sobre Literacia Mediática (GILM), envolvendo a preparação da conferência e a coordenação da operação "7 Dias com os Média".
No que respeita à capacitação de jovens, será promovido o CIS Digital Camp, um programa intensivo dirigido a estudantes do ensino secundário, assim como os CIS Cyber Bootcamps, onde jovens com competências avançadas orientarão novos talentos sob a supervisão de treinadores. Para incentivar a participação de jovens raparigas, será realizado um CIS Cyber Bootcamp específico para este grupo.
A sensibilização através de cursos de e-learning (MOOCs) continuará a ser central, com cinco cursos que abordam temas de cibersegurança, dirigidos ao público em geral. No âmbito do Cybersecurity Challenge PT, será dinamizada uma série de iniciativas de divulgação e competição CTF, incluindo teasers para jovens do ensino secundário e CTF para estudantes universitários. Haverá ainda a disponibilização de uma plataforma de treino, com o objetivo de preparar e selecionar os membros que irão representar Portugal em competições internacionais, como o European Cybersecurity Challenge 2025 e o International Cybersecurity Challenge 2026.
Todas estas atividades serão reforçadas por parcerias com entidades intermunicipais, comunidades de cibersegurança e instituições educativas, com o objetivo de integrar a cibersegurança nos currículos escolares e universitários, promovendo a consciencialização desde cedo. Além disso, serão desenvolvidos materiais educativos específicos e implementados programas de sensibilização em escolas e universidades, consolidando a importância da cibersegurança entre os jovens.

Formação Avançada (FA)

No âmbito da formação disponibilizada pelo CNCS destaca-se o programa de formação avançada em cibersegurança, C-Academy, cujo cumprimento dos objetivos definidos e o alcance das metas estabelecidas no âmbito do PRR será concretizado através do desenvolvimento de várias ações estratégicas ao longo de 2025. Estas consideram o acompanhamento e a operacionalização das formações contratualizadas com as instituições de ensino superior, o fortalecimento de compromissos e parcerias, e o desenvolvimento de soluções para o período pós-PRR. Será dada especial atenção às instituições de ensino superior que, até ao momento, não têm conseguido cumprir os contratos estabelecidos, com o intuito de apoiar e facilitar o progresso. Paralelamente, será promovido um diálogo mais próximo com associações socioprofissionais representativas, como a COTEC ou a CIP, assim como com entidades públicas relevantes, como o IAPMEI, visando formalizar novas parcerias que fortaleçam e expandam as atividades em curso.
A formação a distância, através da plataforma NAU, continuará a ser uma prioridade, assim como a implementação de um roadshow focado na transposição da diretiva NIS 2, ambos cruciais para garantir o cumprimento das metas definidas.
Em perspetiva para o período pós-PRR, será desenvolvido um estudo de viabilidade que permita a criação de um modelo de governança adaptado às necessidades e desafios, assegurando a sustentabilidade e eficiênciada C-Academy.

Observatório de Cibersegurança (OC)

Em 2025, a prioridade do DDI será a de garantir o alinhamento e conformidade com a transposição da diretiva NIS 2, reforçando a segurança digital das organizações em algo que terá reflexos no trabalho do Observatório

de Cibersegurança em particular. No âmbito das suas responsabilidades, o DDI manterá a publicação dos documentos anuais, incluindo o Relatório Riscos e Conflitos 2025 e o Relatório Sociedade 2025, ambos produzidos internamente. Além disso, serão lançados cinco boletins informativos, com temas ainda a definir, e a plataforma de Power BI na página da internet do CNCS será continuamente atualizada e desenvolvida com recursos internos.

Outro foco será a finalização de documentos iniciados em 2024, como os estudos de casos sobre incidentes com vista a criação de materiais didáticos, o estudo com a Comissão Nacional de Proteção de Dados (CNPD) sobre cibersegurança e dados pessoais e o estudo produzido no âmbito do Centro Nacional de Coordenação (NCC) sobre a capacitação das organizações em Portugal. Adicionalmente, será concluído o estudo sobre vulnerabilidades.

Quanto a novos documentos, será desenvolvido um estudo que analisará os incidentes e cibercrimes, particularmente as "cifras negras", fornecendo uma análise aprofundada do impacto de certos serviços do CNCS, bem como uma estimativa dos custos dos incidentes. Este trabalho, de elevada prioridade, será realizado externamente. Outro projeto relevante é a segunda edição do Relatório Ética & Direito, que considerará o novo regime jurídico nacional e europeu. Por fim, será também realizado um estudo que analisará o investimento das empresas em cibersegurança e os custos de conformidade com o novo regime jurídico nacional, reforçando a prioridade de adaptação às novas normativas europeias.

Comunicação e Imagem (CI)

Em 2025, a estratégia de comunicação do CNCS focar-se-á no alinhamento com a sua missão, reforçando a imagem institucional e promovendo o reconhecimento da marca. Serão realizadas campanhas de comunicação para aumentar a visibilidade e credibilidade do CNCS, com ênfase na relação com os meios de comunicação social, através da organização de sessões de esclarecimento e webinars temáticos. Um dos principais objetivos será a atualização e segmentação de contactos de jornalistas, promovendo uma comunicação eficaz e direcionada.

A produção de conteúdos ajustados aos diferentes stakeholders continuará a ser prioritária, com a manutenção do podcast “Comunicar Cibersegurança” e do webinar “Cibertemas”. Paralelamente, serão harmonizadas as peças gráficas institucionais, assegurando uma identidade visual consistente.

A conferência C-DAYS, a realizar-se no Centro de Congressos do Estoril, terá a sua 11ª edição, mantendo-se como o maior evento do CNCS. O evento incluirá sessões técnicas e reuniões estratégicas com diferentes comunidades de cibersegurança, além de uma expansão para novas regiões através da iniciativa C-Days Parceiros.

Na comunicação interna, será implementada uma nova newsletter para promover o envolvimento dos colaboradores, aliada a ações de teambuilding e partilha de informação, fomentando o espírito de missão e a integração dentro do CNCS.

Por fim, o acompanhamento da imagem e identidade do CNCS será assegurado com uma revisão dos modelos visuais e campanhas publicitárias que reforcem a missão da instituição. No âmbito da comunicação de crise, será realizado um exercício institucional em parceria com o Observatório de Cibersegurança, colocando em prática as orientações do Referencial de Comunicação e Crise em Cibersegurança.

OBJETIVOS OPERACIONAIS

DDI_PI105 – Estudo de viabilidade do modelo de governança - C-Academy.

Indicador: Contratação do estudo.

Meta: 30 de setembro

DDI_PI107 – Avaliar a conferência C-DAYS2025.

Indicador: Relatório da conferência aprovado.

Meta: 30 de novembro

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 apoio ao desenvolvimento de capacidades nas organizações é realizado 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)

No âmbito da C-Network, o DCTO garantirá a operacionalização da governação da Rede, tendo em conta o modelo definido e aprovado para todos os Centros de Competências em Cibersegurança (CCC). Tendo ainda em consideração a aquisição de serviços no âmbito da monitorização, gestão material, financeira e de impacto, para além do controlo de qualidade do projeto, o DCTO terá a responsabilidade de garantir a sua boa execução, assim como propor e operacionalizar uma estratégia que permita a sustentabilidade deste projeto após o período de financiamento previsto em PRR. Relativamente ao C-HUB, o DCTO focar-se-á na implementação operacional das atividades ao nível da coordenação e monitorização do projeto, do apoio ao teste de tecnologia, na criação de exercícios e cenários orientados para PMEs e no apoio à capacitação especializada de entidades. Estrategicamente, o DCTO procurará garantir a continuidade deste projeto, através da definição de um modelo de sustentabilidade, após o período de financiamento acordado, bem como a manutenção do selo de excelência enquanto Polo de Inovação Digital Europeu (EDIH).
No que diz respeito ao NCC-PT, o CNCS irá assegurar, em 2025, as atividades de coordenação, monitorização e acompanhamento das ações e decisões tomadas no âmbito do consórcio, funcionar como ligação entre o NCC-PT, o Centro Europeu de Competências em Cibersegurança (ECCC), a Comissão Europeia e outras entidades de interesse, incluindo a participação nas atividades de cooperação no âmbito da rede europeia de NCCs, garantir a criação, registo, manutenção e apoio à comunidade nacional de Cibersegurança. Adicionalmente, o NCC-PT acompanhará a criação e operacionalização do Cluster Nacional de Cibersegurança e procurará lançar um estudo com vista à criação de um fundo de emergência para as entidades da Administração Pública.
O DCTO continuará a promover, em 2025, o planeamento, a organização e a execução de Exercícios de Cibersegurança. À semelhança dos anos anteriores, será assegurada a organização do ExNCS, em moldes e com setores-alvo ainda por definir. Também neste âmbito, será avaliada a possibilidade de desenvolver um "kit de exercícios" (exercise in a box), com o objetivo de disponibilizar às organizações um conjunto de orientações e elementos de treino, de modo a capacitá-las para o planeamento e organização de exercícios internos de Cibersegurança. Adicionalmente, e numa perspetiva de suporte à execução de exercícios de cibersegurança, mas também de capacitação interna, pretende-se dinamizar a plataforma de CyberRange do CNCS, analisando a sua adequabilidade aos objetivos mencionados e desenvolvendo, caso necessário, playbooks adequados. Finalmente, interessa ainda destacar a atividade a desenvolver no âmbito dos serviços de suporte de cibersegurança da ENISA (ENISA Service Support), onde o DCTO continuará a assegurar a execução deste serviço, funcionando como ponto de contacto entre a ENISA, na qualidade de gestora e prestadora do serviço,

e os beneficiários nacionais, com um maior enfoque nas tarefas de avaliação de capacidades, nomeadamente testes de infraestrutura e recursos (testes de penetração).

Comunidades de Cibersegurança (CCS)

No âmbito da criação e dinamização de Centros de Análise e Partilha de Informação (ISACs), em 2025, pretende-se estimular e acompanhar continuamente os ISACS já criados e, por outro lado, proporcionar a operacionalização de novos ISACs setoriais, nomeadamente nos setores dos transportes rodoviário e ferroviário. Também no âmbito da dinamização das comunidades de Cibersegurança, o DCTO continuará a apoiar a Aliança para a Cibersegurança na execução do seu plano de atividades. Em 2025, prevê-se que a Aliança prossiga o desenvolvimento de um conjunto de atividades no âmbito da partilha de conhecimento e capacitação, com maior enfoque na realização de workshops temáticos e em projetos relacionados com a cibersegurança aplicada à cadeia de fornecimento. Adicionalmente, e na sequência de processo iniciado em 2024, será prosseguido o seu alargamento a novas entidades. Finalmente, e com o objetivo de fomentar a colaboração e partilha de boas práticas entre entidades da Administração Pública, o DCTO continuará a assegurar a organização do Fórum de Cibersegurança da Administração Pública Local (FCSAL), integrando entidades intermunicipais e autarquias (e operando numa lógica de coordenação rotativa com as entidades intermunicipais) e irá assegurar a coordenação e dinamização do Grupo de Trabalho em Cibersegurança no âmbito do Conselho para o Digital na Administração Pública. Finalmente, o DCTO continuará a garantir a evolução e a dinamizar a utilização da plataforma C-COM, na qual se prevê integrar todas as comunidades existentes, no decorrer do ano de 2025.

Quadro Normativo de Cibersegurança (QNC)

Na sequência do processo de transposição da diretiva NIS2 atualizar o QNRCS, o qual deverá incluir a disponibilização de uma ferramenta integrada com os seguintes objetivos principais: desenvolvimento de um processo de identificação de riscos setoriais; avaliação de maturidade (evolução do CyberCheckup); atualização do mapeamento entre o Referencial de Competências e a nova versão do QNRCS; apresentação de catálogo de modelos com, pelo menos, cinco políticas de segurança. Numa segunda fase, e com o objetivo de comunicar a estratégia anterior, pretende-se desenvolver um guia de suporte à implementação do novo quadro normativo, no âmbito da capacitação organizacional, que permita orientar as entidades na compreensão das ferramentas e referenciais disponibilizados pelo CNCS. Este guia procurará enquadrar os objetivos do QNRCS e respetivos níveis de garantia, instrumentos de certificação, gestão do risco, notificação de incidentes, etc., bem como a interligação entre cada um deles. Finalmente, e tendo em conta a relevância atribuída à gestão de riscos em cibersegurança, o DCTO continuará a promover a sua adoção e implementação num conjunto de entidades, mantendo a atividade de cooperação já iniciada com a congénere luxemburguesa no sentido de apoiar no desenvolvimento e adaptação da ferramenta Monarc. Adicionalmente, o DCTO dará continuidade ao processo iniciado de gestão de riscos interno em Cibersegurança, em colaboração com o DST e CISO.

OBJETIVOS OPERACIONAIS

DCTO_PI108 – Entidades apoiadas pelos Centros de Competência – controlo final.

Indicador: PRR: Entidades apoiadas, verificável através dos relatórios trimestrais de acompanhamento.

Meta: 1 600.

DCTO_PI109 – Definir 3 níveis de garantia em conformidade com o RJCS2.

Indicador: Documento aprovado com os 3 níveis de garantia.

Meta: 31 de julho.

DEPARTAMENTO DE OPERAÇÕES (DO)

O Departamento de Operações (DO) integra o CERT.PT e assegura a condução da atividade operacional do CNCS em matérias de coordenação da resposta a incidentes e monitorização da atividade e ameaças no ciberespaço de interesse nacional, resultando, também, na 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 DO 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, bem como a investigação e a análise forense sobre esses mesmos incidentes. Neste âmbito são assegurados serviços de gestão e coordenação da resposta a incidentes de cibersegurança no ciberespaço de interesse nacional, de análise, deteção e prevenção de incidentes de cibersegurança no ciberespaço de interesse nacional e produção do Quadro Situacional da Cibersegurança Nacional.

O DO divide a sua atividade em três atividades fundamentais: a reposta a incidentes, a análise de dados de cibersegurança e a produção de dados situacionais. Embora o quadro situacional não seja consubstanciado numa equipa física a relevância do mesmo recolhe esforços de todos os elementos do departamento, podendo assim considerar-se como uma atividade transversal.

Gestão e Coordenação da Resposta a Incidentes (GCI)

A atividade gestão e coordenação da resposta a incidente implica um acompanhamento de todo o ciclo de vida dos incidentes reportados ao CERT.PT, desde a sua notificação ou deteção ao seu encerramento, passando por diversas etapas que podem compreender ações operacionais intermédias, como a análise forense ou a cooperação operacional com outras entidades. Neste âmbito, tal como sucedeu nos anos anteriores, o número de incidentes observados, recolhidos e comunicados ao CERT.PT deverá continuar a sua trajetória ascendente, ainda que num ritmo provavelmente inferior ao verificado no biénio 2023/2024, fruto da estabilização e colocação em serviço de novas fontes e origens de dados durante o ano de 2024.

Ainda assim, este crescimento levará o processamento de incidentes para números de incidentes nunca atingidos, o que forçará um melhoramento na arquitetura de todo o sistema de resposta a incidentes, antecipando-se que se tornará imperativo automatizar muitas das funções que hoje são efetuadas por operadores em sala. Em 2025 será efetuada a desmaterialização ou externalização do serviço de primeira linha, o que permitirá aumentar a capacidade e a qualidade do trabalho dos técnicos atualmente empenhados em tarefas repetitivas e de baixa tecnicidade.

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 prosseguirá um caminho de dotação contínua dos meios técnicos e humanos necessários ao cumprimento desse objetivo sendo para o caso adquiridos mais equipamentos dedicados à área forense e – ao mesmo tempo – contratados novos colaboradores.

Deteção e Prevenção de incidentes (DPI)

No âmbito da deteção e prevenção de incidentes a equipa de Cyber Threat Intelligence (CTI), assegura a monitorização, recolha, análise e partilha de informações sobre riscos e vulnerabilidades, assim como a produção de alertas de cibersegurança e de vulnerabilidades. Está ainda incumbida da identificação de sistemas vulneráveis no ciberespaço nacional.

Neste âmbito, as atividades desenvolvidas têm como prioridade a partilha em tempo útil de informação considerada relevante, como indicadores de comprometimento, com a comunidade nacional e internacional, de forma proativa. 2025 será necessariamente um ano de aposta forte nos mecanismos de deteção e prevenção

de vulnerabilidades e outras ameaças, pelo que continuar-se-á a aposta em meios de inteligência artificial que permitam operacionalizar a totalidade dos dados recolhidos e processados pelo CERT.PT, mais especificamente os dados que já constam das bases de dados do departamento. Ao mesmo tempo será necessário melhorar significativamente a qualidade do Data Lake que suporta toda a atividade do Departamento, para acomodar os dados que chegarão da rede de sensores bem como de outras novas fontes e origens de dados, mantendo tempos de processamento regulares. Para esse efeito será instalado o hardware adequado para o armazenamento de grandes quantidades de dados, garantido o melhoramento simultâneo da capacidade de processamento dos mesmos. Nesse sentido será adquirido equipamento informático com capacidade suficiente para suportar esse esforço. Cumulativamente, continuarão os trabalhos de implementação e alargamento do mecanismo de deteção, acompanhamento e gestão de vulnerabilidades, projeto iniciado em 2024, que terá durante 2025 um período de disseminação por todo o ciberespaço nacional. Da mesma forma prosseguirão os esforços de implementação de um sistema de reputação DNS (DNS RPZ), que se pretende que venha a ser adotado durante 2025 por um número alargado de entidades da comunidade servida pelo CNCS. 2025 será também um ano de instalação do projeto europeu ENSOC, tendo este o seu arranque operacional.

Quadro Situacional da Cibersegurança Nacional (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 o cibersegurança nacional.
Durante 2025 serão operacionalizadas e colocadas em funcionamento as melhorias efetuadas durante o ano anterior, implementando os mecanismos necessários para o lançamento de procedimentos para a criação de novas funcionalidades.
Esta ferramenta, que permite ao CNCS ter visão global do estado do ciberespaço nacional em tempo real num qualquer momento presente, continuará, portanto, a ser desenvolvida durante o ano de 2025.

OBJETIVOS OPERACIONAIS

DO_P127 - Implementar o Sistema Data Lake

Indicador: Sistema Data Lake em funcionamento

Meta: 31 de dezembro

DO_PI128 – Adjudicar a externalização da Equipa de Resposta a Incidentes (ERI).
Indicador: Contrato assinado.

Meta: 31 de julho

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.

Assim, o DRSC, no exercício da função de regulação, 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. Em simultâneo, 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. Assegura também as funções de CISO do GNS / CNCS e garante a prestação de uma gama de outras atividades permanentes, como a representação em fora internacionais, o apoio à Tutela, a cooperação nacional e internacional e a participação em eventos ad hoc.

Regulação (RG)

Em 2025 entrará em vigor um novo regime jurídico da cibersegurança (RJCS), adaptado às disposições estabelecidas na Diretiva NIS 2. Assim, o DRSC promoverá atividades dentro da área da regulação, a nível nacional, relacionadas com a identificação das entidades abrangidas pelo âmbito de aplicação do RJCS, incluindo um roadshow nacional direcionado a gestores de topo destas entidades, a prestar no contexto da C-Academy, e ainda ações informativas específicas sobre o RJCS e normativos associados, tendo como público-alvo a magistratura, procurando o apoio da Procuradoria-Geral da República e do Conselho Superior da Magistratura.

Está previsto o desenvolvimento de regulamentação necessária para a aplicação do RJCS, em colaboração com o Núcleo de Apoio ao Coordenador, nomeadamente na sua vertente jurídica, assim como de regulamentação setorial que se revele necessária, em estreita cooperação com as autoridades setoriais.

Em 2025, o DRSC, dentro da área da regulação, a nível internacional, conduzirá a atividade de liderança do work stream da Saúde no contexto do NIS Coopperation Group e assegurará proactivamente a participação nos work streams a cargo do DRSC, sobretudo os que levem a resultados em sede de regulação e regulamentação.

Supervisão (SV)

Dentro desta área de atividade, perspetiva-se em 2025 o início da atividade de supervisão regular da conformidade com o RJCS, beneficiando da experiência das auditorias piloto ocorridas em 2024 à luz do atual Regime Jurídico de Segurança do Ciberespaço (RJSC).

Prevê-se também o desenvolvimento de ferramentas de suporte à supervisão do RJCS, nomeadamente a reestruturação das bases de dados de contactos das entidades utilizadas pelo CNCS, em estreita articulação com o Departamento de Operações, e uma ferramenta de suporte à supervisão, consistindo num sistema de informação (SI) do DRSC para gestão automatizada da atividade de supervisão, onde se inclui um módulo para gestão das contraordenações e uma plataforma eletrónica para a autoidentificação e qualificação de entidades no âmbito do RJCS. Esta plataforma servirá também como canal preferencial de interação com as comunidades de cibersegurança, incluindo para a notificação de incidentes. Adicionalmente, prosseguir-se-ão os processos de contraordenação iniciados em 2023 e 2024, antecipando-se 2025 como um ano de adaptação a um novo regime jurídico de cibersegurança.

A nível internacional, prevê-se o desenvolvimento de diligências de articulação com autoridades congéneres sobre entidades com atividade transnacional, bem como a realização de todas as atividades atribuídas ao ponto

de contacto único nacional, em particular para fins de aplicação dos artigos 3.º, n.º 5 (notificação à Comissão e ao Grupo de Cooperação do número das entidades essenciais e importantes), 27.º (Registo de entidades) e 37.º (Assistência mútua) da Diretiva NIS 2.

Certificação (CTF)

A área de atividade da certificação da cibersegurança, pautar-se-á no plano nacional, em 2025, pela dinamização da adoção do esquema nacional de certificação de empresas prestadoras de serviços de cibersegurança junto de potenciais interessados, através, por exemplo, da realização de eventos de divulgação do esquema direcionados às empresas prestadoras de serviços de cibersegurança, e ainda pela adaptação do Esquema de Certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança revisto.

No plano internacional, prevê-se contribuir para as discussões no âmbito do desenvolvimento dos esquemas europeus de certificação da cibersegurança, como o EU5G, mas com particular enfoque no EU Cloud Services. O DRSC procurará ainda promover a divulgação e a adoção dos esquemas europeus, como o EU Common Criteria.

CISO GNS/CNCS

No campo da atividade de CISO do GNS/CNCS, para além das avaliações de maturidade semestrais e dos pen test regulares, no seguimento das atividades prosseguidas no ano anterior, em 2025 serão desenvolvidos uma política de gestão de incidentes e um plano de Segurança GNS/CNCS.

DRSC_P122 – Realizar ações de supervisão do RJSC2.

Indicador: Número de auditorias efetuadas.

Meta: 10.

DRSC_PI114 – Desenvolver uma plataforma de autoidentificação e qualificação de entidades abrangidas pelo RJSC2

OP2: (Objetivo operacional do QUAR 2025).

Indicador 2: Prazo de entrada em funcionamento da plataforma de autoidentificação e qualificação de entidades.

Meta: 31 de julho

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)

No âmbito da gestão de sistemas e infraestruturas são asseguradas atividades para assegurar a disponibilização, gestão e manutenção dos sistemas de suporte ao CERT.PT e à rede corporativa do GNS/CNCS. Neste contexto, são também desenvolvidas atividades regulares de apoio à manutenção da infraestrutura, destacando-se a

renovação do parque de servidores, a atualização da infraestrutura de virtualização e diversas operações de manutenção e atualização de software.
A rede informática que suporta o CNCS e GNS foi evoluindo de forma orgânica à medida das necessidades que foram surgindo, estando prevista em 2025 uma restruturação da rede com o objetivo de simplificar a sua gestão, tornando-a mais segura e eficiente.
Ao nível da infraestrutura de virtualização será realizada uma renovação com vista a garantir uma superior capacidade de processamento e armazenamento, condição essencial de forma a albergar a evolução de vários projetos, tais como o PANORAMA ou o guia de transição digital.
O DST em 2025 prevê ainda prestar apoio transversal na identificação e operacionalização de soluções informáticas de suporte à implementação do novo regime jurídico de segurança do ciberespaço na sequência da transposição da Diretiva NIS 2.

Apoio ao Utilizador (AU)

No que diz respeito ao 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.
Concluída a instalação de um novo sistema de pedidos de serviço em 2024, segue-se em 2025 a parametrização com os casos de uso mais comuns, de forma a tornar a resposta aos pedidos mais eficiente.

Security Operation Centre (SOC)

No âmbito da sua atividade, o DST continuará a prestar a base de apoio ao Secuity Operations Centre (SOC), nomeadamente no conjunto alargado de atividades operacionais, como 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 também a monitorização da política de gestão de vulnerabilidades e de patches.

Dando continuidade ao trabalho executado em 2024 com a criação de um agregador de logs, em 2025 prevê-se o desenvolvimento das regras do SIEM para melhor filtrar e tratar a informação que lhe chega de toda a infraestrutura.

OBJETIVOS OPERACIONAIS

DST_G209 – Implementar novo ambiente Green Lake.

Indicador: Hardware (HW) a funcionar no Data Center (DC).

Meta: 30 de junho.

DST_P129 – Implementar das regras do *Security Information and Event Management* (SIEM).

Indicador: Regras implementadas no SIEM.

Meta: 30 de setembro.

RECURSOS HUMANOS

A estrutura de recursos humanos do GNS e do CNCS compreende militares das Forças Armadas (FA) e da Guarda nacional Republicana (GNR) e pessoal das Forças de Segurança (PSP), disponibilizado e remunerado pelos serviços de origem (FA, GNR e PSP), e pessoal civil, proveniente quer do setor público quer do setor privado.
Em 01 de janeiro de 2024 o GNS dispunha de 156 postos de trabalho previstos no mapa de pessoal, considerando um incremento de 33 novos postos de trabalho dos quais 31 a afetar ao CNCS e 2 ao GNS, 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, , 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 2025 irá prosseguir-se o esforço de recrutamento de pessoal, tendo sido previsto no mapa um acréscimo de 3 postos de trabalho para o GNS, 1 Consultor para a Informática e 2 Assistentes Técnicos que permitam fazer face ao incremento das atribuições do CNCS, em diferentes áreas e muito por força da Norma Europeia NIS2, assim afigura-se como necessário, para que o GNS/CNCS assegure as suas atribuições, o preenchimento de 159 postos de trabalho.
O quadro seguinte projeta, de acordo com o Mapa de Pessoal aprovado para 2025 (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)	64	1
Forças de Segurança (GNR/PSP)	10	0
Civis	14	70
Sub Totais	**88**	**71**
TOTAL	**159**	

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	5	10
Técnicos		54
Assistentes Técnicos	5	1
Assistentes Operacionais	2	-
Sub Totais	**88**	**71**
TOTAL	**159**	

RECURSOS FINANCEIROS

O Orçamento do Estado 2025, conforme o seguinte quadro, foi planeado de Receitas de Impostos (Fonte de Financiamento (FF) 311) para o GNS (Atividade 231) o montante de 1.272.331 e para o CNCS (Atividade 171) o montante de 5.245.801€, e em Receitas Próprias (FF 531) foi planeado para o GNS (Atividade 231) o montante de 1.580.900,00€, totalizando 8.099.032€.

Funcionamento	FF 311 Atividade 231 GNS	Agrupamento 01 - Pessoal	801.726,00€
		Agrupamento 02 - Bens e Serviços	350.000,00€
		Agrupamento 07 - Despesas Capital	120.605,00€
		Subtotal 231	*1.272.331,00€*
	FF 311 Atividade 171 CNCS	Agrupamento 01 - Pessoal	3.317.749,00€
		Agrupamento 02 - Bens e Serviços	1.611.556,00€
		Agrupamento 07 - Despesas Capital	316.496,00€
		Subtotal 171	*5.245.801,00€*
		Total FF 311	6.518.132,00 €
	FF 513 Atividade 231 GNS	Agrupamento 01 - Pessoal	0,00€
		Agrupamento 02 - Bens e Serviços	1.091.377,00€
		Agrupamento 06 - Reserva	39.523,00 €
		Agrupamento 07 - Despesas Capital	450.000,00€
		Total FF 513	1.580.900,00 €
		Total FF 311 + FF513	8.099.032,00 €

Para 2025, foram planeados os projetos que constam no Anexo D 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 551.652,30€, sendo cerca de 530.802,30€ resultante do PRR e o restante valor, cerca de 20.850,00€, suportado pelo orçamento de funcionamento de 2025.

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 2025, 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 XXIV 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 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, 18 de dezembro de 2024

O DIRETOR-GERAL

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2025.02.12 16:09:46 Z

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

ANEXO B – PLANO DE FORMAÇÃO DO CNCS

GNS Gabinete Nacional de Segurança PORTUGAL

CNCS Centro Nacional de Cibersegurança PORTUGAL

PÁGINA DEIXADA EM BRANCO

ANEXO C - QUAR

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

ANEXO D – PROPOSTA DE ORÇAMENTO

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

ANEXO E – MAPA DE PESSOAL

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

ANEXO F – CÓDIGO DE ÉTICA E CONDUTA

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

PÁGINA DEIXADA EM BRANCO

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

GNS
Gabinete Nacional de Segurança
PORTUGAL

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

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