

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

Plano de Atividades

2023

PÁGINA DEIXADA EM BRANCO



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

Relatório de Atividades de 2023

ÍNDICE

1.	SUMÁRIO EXECUTIVO	5
2.	NOTA INTRODUTÓRIA	7
3.	ESTRATÉGIA E OBJETIVOS	9
4.	ATIVIDADES PREVISTAS E RECURSOS	11
4.1.	Atividades Previstas.....	11
4.1.1.	GABINETE NACIONAL DE SEGURANÇA	11
4.1.1.1.	DEPARTAMENTO DE INSPEÇÃO AUDITORIA (IA)	11
4.1.1.1.1.	OBJETIVOS OPERACIONAIS	11
4.1.1.1.2.	INDICADORES DE ATIVIDADE	11
4.1.1.2.	DEPARTAMENTO DE DOCTRINA E FORMAÇÃO (DF).....	11
4.1.1.2.1.	OBJETIVOS OPERACIONAIS	12
4.1.1.2.2.	INDICADORES DE ATIVIDADE	12
4.1.1.3.	DEPARTAMENTO DE GESTÃO DA INFORMAÇÃO CLASSIFICADA E CRIPTOGRAFIA (GICC)	13
4.1.1.3.1.	OBJETIVOS OPERACIONAIS	13
4.1.1.3.2.	INDICADORES DE ATIVIDADE	15
4.1.1.4.	DEPARTAMENTO DE SEGURANÇA DIGITAL, TECNOLÓGICA E DE INFRAESTRUTURAS (SDTI). 16	
4.1.1.4.1.	OBJETIVOS OPERACIONAIS	17
4.1.1.4.2.	INDICADORES DE ATIVIDADE	19
4.1.1.5.	DEPARTAMENTO DE CREDENCIAÇÃO	21
4.1.1.5.1.	OBJETIVOS OPERACIONAIS	21
4.1.1.5.2.	INDICADORES DE ATIVIDADE	22
4.1.1.6.	SERVIÇO DE INFORMÁTICA, REDES E COMUNICAÇÕES (IRC).....	22
4.1.1.6.1.	OBJETIVOS OPERACIONAIS	22
4.1.1.6.2.	Indicadores de Atividade	23
4.1.1.7.	NÚCLEO DE APOIO À DIREÇÃO (NAD)	24
4.1.1.7.1.	OBJETIVOS OPERACIONAIS	24
4.1.1.8.	SERVIÇO DO OFICIAL DE SEGURANÇA (OF SEG)	25
4.1.1.8.1.	OBJETIVOS OPERACIONAIS	25
4.1.2.	CENTRO NACIONAL DE CIBERSEGURANÇA	27
4.1.2.1.	DEPARTAMENTO DE DESENVOLVIMENTO E INOVAÇÃO (DDI)	27
4.1.2.1.1.	OBJETIVOS OPERACIONAIS	29
4.1.2.2.	DEPARTAMENTO DE CAPACITAÇÃO TÉCNICA (DCTO)	30
4.1.2.2.1.	OBJETIVOS OPERACIONAIS	31



PRESIDÊNCIA DO CONSELHO DE MINISTROS
Gabinete Nacional de Segurança
Centro Nacional de Cibersegurança

Relatório de Atividades de 2023

4.1.2.3. DEPARTAMENTO DE OPERAÇÕES (DO)	32
4.1.2.3.1. OBJETIVOS OPERACIONAIS	33
4.1.2.4. DEPARTAMENTO DE REGULAÇÃO, SUPERVISÃO E CERTIFICAÇÃO (DRSC)	34
4.1.2.4.1. OBJETIVOS OPERACIONAIS	36
4.1.2.5. DEPARTAMENTO DE SERVIÇOS TÉCNICOS(DST)	37
4.1.2.5.1. OBJETIVOS OPERACIONAIS	38
5. RECURSOS HUMANOS	39
5.1. RECURSOS HUMANOS	39
5.1.1. MAPA DISCRIMINATIVO	39
5.2. RECURSOS FINANCEIROS	40
5.2.1. VALORES INSCRITOS/PROPOSTOS NO OE-2023	40
6. PLANO DE FORMAÇÃO	45
7. MEDIDAS DE MODERNIZAÇÃO ADMINISTRATIVA	45
8. PUBLICIDADE INSTITUCIONAL	46
ANEXOS	47
MAPA ESTRATÉGICO	49
PERSPETIVA GENÉTICA	53
PERSPETIVA DE PROCESSOS	57
PERSPETIVA DOS PUBLICOS DE INTERESSE	61
OBJETIVOS ESTRATÉGICOS E OPERACIONAIS	3
MAPA DE PESSOAL - 2023	77
PLANO DE FORMAÇÃO PARA 2023	77
QUAR 2023	77

1. SUMÁRIO EXECUTIVO

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

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

Relativamente ao CNCS, ter-se-á, dentro do possível, de prosseguir com o incremento da equipa afeta ao Centro, ainda que se configure premente adequar a Lei Orgânica para conferir maior flexibilidade ao recrutamento, num quadro de grande procura por pessoas com competências na área da cibersegurança, quer no setor público quer, sobretudo, no setor privado.

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

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

Em 2023, pretende-se levar a efeito um conjunto de ações que visam reforçar a consolidação dos projetos e processos iniciados no período 2020 a 2022, nomeadamente a prossecução da desmaterialização dos processos internos e a consolidação da estrutura e dos processos inspetivos executados pelo GNS, visando uma maior proximidade às entidades sujeitas a inspeção.

Para o efeito, é indispensável um adequado nível e maturidade de colaboradores, pelo que é necessário a otimização dos recursos humanos, sendo objetivo do GNS/CNCS atingir, no final de 2023, um quantitativo global de 122 trabalhadores, dos quais 40 no Centro Nacional de Cibersegurança (CNCS).

Em termos financeiros, a dotação inicial do orçamento de funcionamento do GNS/CNCS é de € 3.597.163,00 dos quais € 2.715.552,00 são respeitantes à atividade do CNCS. No âmbito do Plano de Recuperação e Resiliência está previsto um investimento de € 14.295.060,00€. A Lei do OE-2023 e o subsequente decreto-lei de execução orçamental irão, por certo, 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 2023.

Em conclusão, para o ano de 2023, o foco será a execução das medidas e marcos/metast do investimento TD C19-i03 do PRR planeadas para este ano, retendo a flexibilidade suficiente para uma rápida adaptação à volatilidade da envolvente geoestratégica. No que ao atual plano estratégico diz respeito deverá prosseguir-se com um esforço especial em quatro áreas, designadamente:

1. Capacitar os públicos de interesse para os desafios da sociedade do conhecimento;
2. Robustecer a capacidade de conhecimento do ciberespaço relevante e de proteção da sociedade;
3. Modernizar a forma como prestamos o serviço e somos percecionados pelos nossos públicos de interesse;
4. Investir na qualificação e no bem-estar dos colaboradores.

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

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 alta reputação percecionada pelos públicos de interesse no âmbito do cumprimento da missão institucional, com a capacidade para se adaptarem às condições da mudança constante, pensando como organizações 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, procurando fazer diferente, criando 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 2023, o GNS/CNCS pretende dar continuidade e concluir um conjunto de ações, de grande visibilidade externa, prosseguindo com a continuidade da regulamentação setorial do regime jurídico de Segurança do Ciberespaço (Lei nº 46/2018, de 13 de agosto) e a implementação dos respetivos mecanismos de supervisão, bem como da implementação da componente nacional do mecanismo europeu de certificação em Cibersegurança, previsto no Regulamento (UE) 2019/881; no âmbito da ação externa, a promoção de sessões de discussão pública do Projeto de Lei de Segurança da Informação Classificada (LSIC); concluir a reformulação do modelo de formação sobre gestão do ciclo da vida da Informação Classificada (IC), passando-se de um modelo exclusivamente presencial para um 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, implementando um Programa de Formação Avançada em Cibersegurança, 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, do Polo de inovação digital em CS; no âmbito da simplificação da interação com os públicos de interesse, concluir a implementação dos novos sistemas de Segurança Eletrónica da Informação (SEIF) e de Gestão do Ciclo de Vida de Material Cripto (SCRIPTO) e continuar a capacitar a Equipa Nacional CERT.PT com os instrumentos e as ferramentas necessárias para incrementar a sua capacidade de operar e comunicar com a comunidade e autoridades públicas de cibersegurança.

Durante o ano de 2023 será dada continuação ao ambicioso programa nacional de formação avançada em cibersegurança, designado por *C-Academy*, iniciado em 2022 e que será o instrumento de requalificação de quadros especializados, Empresas e Administração Pública em cibersegurança nas mais diversas vertentes. A materialização da *C-Academy* irá assentar na elaboração de protocolos com as instituições de ensino nacionais.

3. 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 2023, tendo em conta as respetivas natureza, missão e atribuições.

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

Os objetivos estratégicos definidos foram agrupados segundo três perspetivas:

- A perspetiva dos **Públicos de Interesse**, onde se procura ter um correto conhecimento, compreensão e interpretação daquilo a que os diversos públicos servidos pelo GNS e pelo CNCS dão realmente importância, entregando os produtos e serviços em alinhamento com a missão e a perceção das reais necessidades.
- A perspetiva dos **Processos**, onde se identificam os procedimentos que relevam para que a organização alcance a excelência na forma como satisfaz os seus públicos de interesse e como acrescenta valor. O princípio fundamental é o de gerar produtos ou prestar serviços de melhor qualidade com o menor custo, na linha da melhor eficiência.
- A perspetiva da **Genética**, que incorpora a geração e retenção dos meios necessários para edificar capacidades de forma a melhorar a atuação da organização, de modo a viabilizar uma adaptação à envolvente, a antecipação às mudanças, e a melhoria constante dos conhecimentos dos seus recursos, como forma de consolidação das novas capacidades adquiridas.

O mapa estratégico, em anexo A, é uma ferramenta visual para definir, representar e comunicar a estratégia geral de uma organização. Este mapa fornece um retrato fiel dos objetivos ou das metas da organização e as ações planeadas para atingir essas metas. Os objetivos estratégicos definidos decompõem-se em linhas de ação que visam prosseguir com a edificação equilibrada de capacidades, incluindo a respetiva sustentação, prosseguir com a otimização processual e organizacional, e empregar as capacidades para melhor cumprir a missão do GNS/CNCS.

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

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

No âmbito da sua missão, as principais atividades desenvolvidas pelo GNS são a credenciação de: (i) segurança de pessoas singulares ou coletivas para administração de informação classificada; (ii) entidades de certificação eletrónica do Estado; (iii) segurança a entidades para o exercício de atividades industriais, tecnológicas e de investigação; (iv) segurança nacional às empresas de comércio e indústria de bens e tecnologias militares, de certificação de segurança a produtos e sistemas de comunicações, de informática e de tecnologias de informação classificada, certificação das entidades gestoras de plataformas eletrónicas de contratação pública e supervisão da implementação do regulamento 910/2014 da UE. Relativamente ao CNCS, no âmbito da sua missão, as principais atividades centram-se no desenvolvimento das capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção destinadas a fazer face a incidentes de cibersegurança e ciberataques, no processo de regulamentação da Lei 46/2018 de 13 de agosto que transpõe a Diretiva de Segurança das Redes da Informação (Diretiva SRI) para a legislação nacional, e na coordenação do plano de ação da ENSC 2019-2023. Com a publicação do DL 65/2021 de 30 de julho, que Regulamenta o Regime Jurídico

da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança, o CNCS reforçou as suas competências enquanto Autoridade Nacional de Certificação de Cibersegurança.

Conforme acima referido, foi definido um conjunto de objetivos estratégicos para o triénio 2023/2026, e que constam no mapa estratégico. A avaliação de desempenho de cada serviço assenta num quadro de avaliação e responsabilização (QUAR), onde constam os objetivos anualmente fixados e, em regra, hierarquizados. O critério de seleção dos objetivos e indicadores a integrar o QUAR é, em primeira instância, o da consecução da missão da organização.

Para 2023, foram selecionados, para constarem no QUAR, os seguintes objetivos estratégicos:

- Capacitar os públicos de interesse para os desafios da sociedade do conhecimento;
- Robustecer a capacidade de conhecimento do ciberespaço relevante e de proteção da sociedade;
- Modernizar a forma como prestamos o serviço e somos percecionados pelos nossos públicos de interesse;
- Investir na formação e no bem-estar dos colaboradores.

Destes objetivos estratégicos decorrem 2 do GNS, 2 do CNCS e os obrigatórios objetivos operacionais, inscritos no QUAR-2023, cuja concretização será obtida mediante a realização das atividades de cada uma das unidades orgânicas do GNS e CNCS.

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

4. ATIVIDADES PREVISTAS E RECURSOS

4.1. Atividades Previstas

Para a concretização dos objetivos estratégicos estabelecidos, a ação da organização concentra-se em 45 objetivos operacionais. Para se atingirem os objetivos definidos, torna-se necessário desenvolver um conjunto de ações cuja concretização permite atingir os objetivos fixados, operacionais e estratégicos.

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.

4.1.1. GABINETE NACIONAL DE SEGURANÇA

4.1.1.1. DEPARTAMENTO DE INSPEÇÃO 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.

4.1.1.1.1. OBJETIVOS OPERACIONAIS

IA_G201- Desenvolver um Sistema de Gestão e Controlo da Atividade Inspeciva e de Auditoria (GAIA).

Indicador: Percentagem de desenvolvimento do Projeto (De acordo com “Plano de Desenvolvimento e Implementação”.

Meta: 100% do plano.

4.1.1.1.2. INDICADORES DE ATIVIDADE

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

Indicador: Número de Inspeções.

Meta: 20.

IA102- Realizar e coordenar a atividade inspetiva internacional.

Indicador: Número de Inspeções a Embaixadas e Postos Diplomáticos.

Meta: 3.

4.1.1.2. DEPARTAMENTO DE DOCTRINA 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 2023, o desenvolvimento e implementação de formação, no formato e-learning, para o refrescamento dos temas abordados no Curso de Introdução à Segurança da Informação Classificada (CISIC), destinada à frequência pelos sujeitos que necessitem de ver renovada a sua credenciação de segurança.

Em simultâneo, estabelecem-se os objetivos de operacionalização da formação e treino no âmbito do sistema seguro de troca de informação entre os órgãos de segurança e a introdução de casos práticos na formação de forma a contribuir, para o cumprimento das políticas de segurança, procurando paralelamente, manter os elevados índices de satisfação.

O Departamento de DF elege e destaca nas suas atividades para 2023, o incremento da cultura de segurança e o desenvolvimento e atualização das respetivas políticas, com a materialização de ações de formação e sensibilização realizadas por todo o país e, através do seu núcleo de Doutrina, a representação do GNS nos fóruns onde as políticas de segurança são discutidas, nomeadamente nos Comitês (Security Committee) da NATO e da EU, promovendo a atualidade de todo o normativo nacional (Normas Técnicas). Desenvolve também, as atividades não discriminadas relativas à celebração e atualização de acordos bilaterais com outros estados para a proteção mútua de IC. A DF persegue ainda a atividade de discussão pública da atualização do Quadro Legal do GNS, tema inadiável e que almeja a substituição dos SEGNAC (Segurança Nacional) vigentes, na forma de Resoluções de Concelhos de Ministros.

4.1.1.2.1. OBJETIVOS OPERACIONAIS

DF_P101 – Disponibilizar um curso sobre Segurança da Informação Classificada, num modelo de e-learning.

Indicador: Disponibilização do curso na plataforma e-learning.

Meta: 29 de dezembro.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.1- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.1.4- Qualificação de pessoas e organizações para poderem tratar informação, para concretização do objetivo, inscrito no contrato do PRR, como meta 1362 – Qualificação de pessoas e organizações para poderem tratar informação, visando disponibilizar 6 cursos até ao 1T de 2026 e reconhecer 2 deles.

DF_PI101 - Promover ganhos de eficiência no domínio da formação interna e externa (% índice de satisfação) **(Objetivo operacional do QUAR 2023 – Relevante).**

Indicador 1: Índice de satisfação médio (em %) dos formandos que frequentaram ações de formação ministrada pelo GNS.

Meta: 85%.

4.1.1.2.2. INDICADORES DE ATIVIDADE

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

Indicador: Previstas 30 ações (10 – GNS e 20 – CNCS). Número de ações previstas.

Meta: 24.

IA104 – Discussão na Assembleia da República.

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

Indicador: Prevê-se a realização de uma sessão.

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

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

IA106 –Acordos.

Indicador: Assinatura de Acordos bilaterais (Croácia, Chipre, Bósnia e Herzegovina, Geórgia, Macedónia do Norte, Sérvia, Reino Unido, Argélia, Índia, Qatar e Bélgica). Tempo de elaboração dos acordos.

4.1.1.3. 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.

4.1.1.3.1. OBJETIVOS OPERACIONAIS

GICC_PI102- Otimizar a utilização das instalações do "SubRegisto as a Service" (**Objetivo operacional do QUAR 2023 – Relevante**).

Indicador 1: Conclusão das melhorias nas infraestruturas do "SubRegisto as a service".

Meta: 30 de julho.

Indicador 2: Inicial Operability Capability (IOC).

Meta: 31 de outubro.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente, como submedida TD C19 i03.2.3-Sub-Registo as a Service, para concretização do objetivo, inscrito no contrato do PRR, como meta 1366 – Operacionalizar o serviço "SubRegisto as a service", a qual se conclui com a alteração da portaria.

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

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

Meta: 6 entidades.

Indicador 2: Processo de certificação do eSEIF.

Meta: 50% do processo de cerificação.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.2.2- Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada), para concretização do objetivo, inscrito no contrato do PRR, como meta 1365 – Aumentar o número de entidades utilizadoras do Sistema de Segurança Eletrónica da Informação (SEIF), visando certificar 34 entidades utilizadoras do Sistema até 2025.

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

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

Meta: 50%. do desenvolvimento.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.2.2- Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada), para concretização do objetivo determinado pela meta 1365 – Aumentar o número de entidades utilizadoras do Sistema de Segurança Eletrónica da Informação (SEIF), visando certificar 34 entidades utilizadoras do Sistema até 2025.

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

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

Meta: 1 de fevereiro.

Indicador 2: Desenho da rede Software Defined Network (SDN) com capacidade *Quantum Key Distribution* (QKD) e desenho da máquina de cifra com QKD (Work Package 5 (WP5) e Work Package 6 (WP6) e estudo da industrialização da máquina de cifra (WP6.3).

Meta: 30 de setembro.

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

Meta: 28 de fevereiro

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.2.4- Capacidade Criptográfica Nacional, para concretização do objetivo, inscrito no contrato do PRR, como meta 19.8 – Garantir a adoção da solução criptográfica portuguesa pelas autoridades públicas, cuja meta será a receção do equipamento criptográfico por parte de 150 de autoridades públicas em 2026.

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: 1 de junho.

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

Meta: 100%.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.2.2- Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada), para concretização do objetivo, inscrito no contrato do PRR, como meta 1365 – Aumentar o número de entidades utilizadoras do Sistema de Segurança Eletrónica da Informação (SEIF), visando certificar 34 entidades utilizadoras do Sistema até 2025.

GICC_P106 – Desenvolvimento evolutivo da máquina de cifra HSM-T2 para nova versão 2.1. **(Objetivo operacional do QUAR 2023 – Relevante).**

Indicador 1: Desenho de novo algoritmo de chaves internas mais robusto, ligação externa para programação e carregamento de chaves, botão ZEROID, e revestimento de proteção para operações em ambientes desfavoráveis.

Meta: 1 de outubro

Indicador 2: Plano de industrialização para o fabrico de 100 unidades.

Meta: 29 de dezembro

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.2.4- Capacidade Criptográfica Nacional, para concretização do objetivo, inscrito no contrato do PRR, como meta 19.8 – Garantir a adoção da solução criptográfica portuguesa pelas autoridades públicas, visando o desenvolvimento e entrega de 150 máquinas de cifra até ao primeiro trimestre de 2026.

4.1.1.3.2. INDICADORES DE ATIVIDADE

IA107 – Operacionalização do HSMT 2.0.

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

Meta: 31 de janeiro.

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 publicas apoiadas.

Meta: 5.

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

Indicador: Registrar 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.

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

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

Áreas de competência do Departamento

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

Segurança Tecnológica

Compete à Segurança Tecnológica, avaliar, certificar e acreditar a segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada, assim como, proceder à realização de limpezas eletrónicas em áreas sensíveis onde seja tratada informação com necessidades especiais de segurança.

Segurança das Infraestruturas

Contribui para a Acreditação/Certificação das infraestruturas, dos sistemas ou equipamentos de segurança que conferem proteção física aos locais ou SIC que processem, arquivem ou transmitam informação

classificada, competindo-lhe ainda colaborar nas inspeções periódicas aos órgãos de segurança sob responsabilidade portuguesa, no território nacional e no estrangeiro, detentores de informação classificada.

Segurança do Espaço

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

Serviços de Confiança

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

A atividade do SDTI para 2023 traduz-se assim nos seguintes conjuntos de objetivos de operacionais e atividades correntes:

4.1.1.4.1. OBJETIVOS OPERACIONAIS

SDTI_P107- Implementar o Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada.

Indicador: Prazo para apresentação da proposta.

Meta: 30 de junho.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente, como submedida TD C19 i03.2.1- Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, para concretização do objetivo, inscrito no contrato do PRR, como meta 1364 - Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, visando incrementar, certificar e acreditar 24 sistemas.

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

Indicador 1: Prazo para manifestação de necessidades das contramedidas eletrónicas para o domínio acústico.

Meta: 31 de março.

Indicador 2: Prazo para a apresentação do manual de procedimentos relativos ao planeamento de desenvolvimento de operações de limpeza eletrónica.

Meta: 30 de novembro.

Indicador 3: Prazo para manifestação de necessidades de ferramentas de acreditação e auditoria de sistemas de informação classificada.

Meta: 30 de julho.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente como, submedida TD C19 i03.2.1- Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, para concretização do objetivo, inscrito no contrato do PRR, como meta 1364 - Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, visando incrementar, certificar e acreditar 24 sistemas.

SDTI_P109- Reforçar a capacidade de certificação de sistemas, equipamentos e produtos – certificação TEMPEST, através da capacitação do Centro Laboratorial e Normalização (CLN) da ANACOM e implementação do respetivo plano de certificação.

Indicador: Implementar plano de certificação TEMPEST.

Meta: 29 de setembro.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19-i03.2 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente como, submedida TD C19 i03.2.1- Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, para concretização do objetivo, inscrito no contrato do PRR, como meta 1364 - Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, visando incrementar, certificar e acreditar 24 sistemas.

SDTI_P110 - Edificação do centro de operações da Competent Public Regulated Service Authority (CPA).

Indicador 1: Deployment pela EUSPA da rede GRON (Galileo Robust Operational Network) no centro de operações da CPA.

Meta: 31 de junho.

Indicador 2: Formação de 2 operadores da CPA.

Meta: 31 de julho.

Indicador 3: Emissão do Statement of Compliance das salas e infraestruturas do GNS, para receber o POCP.

Meta: 30 de abril.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente, como submedida TD C19 i03.2.4- Capacidade Criptográfica Nacional, para concretização do objetivo, inscrito no contrato do PRR, como meta 19.8 - Garantir a adoção da solução criptográfica portuguesa pelas autoridades públicas, , cuja meta será a receção do equipamento criptográfico por parte de 150 de autoridades públicas em 2026.

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

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

Meta: 31 de agosto

Indicador 2: Certificação do Software aplicacional.

Meta: 29 de dezembro.

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

Meta: 29 de setembro

Indicador 4: Digitalização de 20.000 processos de credenciação.

Meta: 29 de dezembro

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03 - Projeto 2 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente como, submedida TD C19 i03.2.5- Certificar e implementar um modelo de preservação digital de informação com requisitos especiais de segurança, para concretização do objetivo, inscrito no contrato do PRR, como meta 1368 - Certificar e implementar um modelo de preservação digital de informação com requisitos especiais de segurança.

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

Indicador: Realização de Prova de Conceito.

Meta: 31 de novembro.

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

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

Meta: 31 de março.

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

Meta: 29 de setembro.

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

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

Meta: 30 de junho.

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

Meta: 31 de março.

4.1.1.4.2. INDICADORES DE ATIVIDADE

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

Indicador: 5.

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

Indicador: 5.

IA117- Número de avaliações de Zoning.

Indicador: 6

IA118- Número de Limpezas Eletrônicas.

Indicador: 6

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

Indicador: 2

IA120 - Inspeccionar os sites nacionais da área do espaço (EGNOS, Galileo, SST, etc.) e elaborar os respectivos processos de acreditação;

Indicador: 3

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

Indicador: 4

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

Indicador: 80

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

Indicador: 4

IA124 - Auditorias/inspeção TSP (Regulamento eIDAS).

Indicador: 4

IA125 - Atualização da TSL (Trusted List).

Indicador: 4.

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

Indicador: 2

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

Indicador: 10

4.1.1.5. 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 específicas 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) e *EEAS Expert meeting on Personnel Security Clearance* da EU, concorrerão para atingir os objetivos operacionais definidos para 2023.

O departamento de credenciação irá ainda apoiar o desenvolvimento do CRESO +, prestando o apoio técnico-funcional para a concretização do objetivo operacional NAD_G202 — Desenvolvimento de novas funcionalidades e melhorias do sistema CRESO. Esse apoio será materializado na participação na elaboração do caderno de análise e de especificações dos testes, tendo em vista a sua completa operacionalização, validando os requisitos técnicos constantes do Caderno de Encargos e identificando possíveis anomalias do sistema.

4.1.1.5.1. OBJETIVOS OPERACIONAIS

DC_P301- Garantir a desmaterialização dos processos de credenciação submetidos (pessoas singulares e coletivas).

Indicador: Percentagem dos processos desmaterializados.

Meta: 80%.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente como submedida TD C19 i03.2.6- Credenciações de segurança (CRESO), para concretização do objetivo, inscrito no contrato do PRR, como meta 1369 - Desmaterializar processos de credenciação de pessoas coletivas e singulares, visando desmaterializar 90% dos processos de credenciação.

DC_P302- Estabelecer protocolos com Entidades Nacionais que podem colaborar nos processos de investigação de segurança a pessoas coletivas e pessoas singulares.

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

Meta: 2.

4.1.1.5.2. INDICADORES DE ATIVIDADE

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

Indicador: Número de reuniões.

Meta: 2 (uma por semestre).

IA129 – Credenciações e investigações de segurança em 2022.

Indicador 1: Número credenciações de segurança de pessoas singulares.

Meta: 6000.

Indicador 2: Número credenciações de segurança de pessoas coletivas.

Meta: 100.

4.1.1.6. 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.

4.1.1.6.1. OBJETIVOS OPERACIONAIS

IRC_P115- Implementação do *Multi Factor Authentication* (MFA).

Indicador: Implementação do Final Operational Capability (FOC).

Meta: 31 de março.

IRC_P116- Implementação do *Dual Boot*.

Indicador: Implementação do FOC.

Meta: 30 de abril.

IRC_P117- Atualização do hardware da atual Rede Interna para futura integração na Rede Classificada ÉGIDE.

Indicador 1: Data término de validação da arquitetura para a Rede ÉGIDE.

Meta: 31 de março.

Indicador 2: Percentagem de Edificação da Rede Égide, grupo criptografia dos segmentos High, Low Level e capilaridade eSEIF.

Meta: 25%.

Risco: Demora na entrega de equipamentos.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.1- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente como, submedida TD C19 i03.2.1- Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas, para concretização do objetivo, inscrito no contrato do PRR, como meta 1364 - Incrementar a

certificação e a acreditação de segurança de sistemas e infraestruturas, visando incrementar, certificar e acreditar 24 sistemas.

IRC_PI103- Implementação do “Disaster Recovery”.

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

Meta: 31 de março

Risco: capacidade de resposta do EMGFA.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2 – Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, identificada internamente como, submedida TD C19 i03.2.2 – Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada), inscrito no contrato do PRR, como meta 1365 - Aumentar o número de entidades utilizadoras do Sistema de Segurança Eletrónica da Informação (SEIF), visando incrementar, certificar e acreditar 24 sistemas.

IRC_PI104- Atualização de funcionalidades na Gestão Documental

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

Meta: 31 de agosto.

4.1.1.6.2. 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.

4.1.1.7. 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.

4.1.1.7.1. OBJETIVOS OPERACIONAIS

NAD_P303- Implementar o Quadro Nacional de Cibersegurança e transformar o atual modelo de coordenação da cibersegurança e da segurança da informação, alcançando a *Initial Operability Capability* (IOC) do modelo.

Indicador: A elaboração do Plano para a IOC.

Meta: Alcançar o IOC até 31 março.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.3- Implementar o quadro nacional de cibersegurança, identificada internamente como, submedida TD C19 i03.3.5- Modelo Integrado e Interoperável de Governação para a Segurança dos Dados, da Informação e do Conhecimento, para concretização do objetivo, inscrito no contrato do PRR, como meta 1377 - Alcançar a Inicial Operability Capability (IOC) do modelo de governação colaboração e partilha de capacidades para a segurança dos dados, da informação e do conhecimento (modelo aprovado).

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

Indicador: Taxa de execução da implementação das novas funcionalidades.

Meta: 70%

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.2- Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente como submedida TD C19 i03.2.6- Credenciações de segurança (CRESO), para concretização do objetivo, inscrito no contrato do PRR, como meta 1369 - Desmaterializar processos de credenciação de pessoas coletivas e singulares, visando desmaterializar 90% dos processos de credenciação.

NAD_G203 — Promover a cultura organizacional através da motivação dos trabalhadores (Nº de atividades) **(Objetivo operacional do QUAR 2023 – Relevante).**

Indicador: Número de atividades realizadas.

Meta: 2.

NAD_G301 – Elaboração do Estudo Prévio para a Requalificação e habilitação das novas instalações do GNS/CNCS.

Indicador: Data de entrega do Programa Preliminar.

Meta: 31 de maio.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.4- Criar as condições físicas e tecnológicas, identificada internamente como submedida TD C19 i03.4.1- Recuperação e requalificação de infraestruturas e instalação dos serviços, para concretização do objetivo, inscrito no contrato do PRR, como meta 1380 - Assegurar a aprovação do projeto para dotar as instalações do GNS/CNCS com as condições necessárias ao cumprimento dos requisitos especiais e específicos de segurança, de forma resiliente, sustentável e inteligente, visando a entrega do projeto para dotar as instalações com os requisitos especiais e específicos de segurança.

NAD_G302 – 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 julho.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.4- Criar as condições físicas e tecnológicas, identificada internamente como submedida TD C19 i03.4.1- Recuperação e requalificação de infraestruturas e instalação dos serviços, para concretização do objetivo, inscrito no contrato do PRR, como meta 1380 - Assegurar a aprovação do projeto para dotar as instalações do GNS/CNCS com as condições necessárias ao cumprimento dos requisitos especiais e específicos de segurança, de forma resiliente, sustentável e inteligente, visando a entrega do projeto para dotar as instalações com os requisitos especiais e específicos de segurança.

4.1.1.8. 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.

4.1.1.8.1. OBJETIVOS OPERACIONAIS

NAD_G303 – Reforçar a Segurança Física das instalações.

Indicador 1: Resolução de anomalias no Sistema de Deteção de Intrusão (SDI).

Meta: 30 de junho.

Indicador 2: Reforço da capacidade de leitura e fiabilidade do Sistema de Controlo de Acessos (SCA) nos pontos críticos e de maior movimento.

Meta: 31 de outubro.

Indicador 3: Ampliação da cobertura do Sistema de Videovigilância (CCTV) no GNS/CNCS.

Meta: 31 de outubro.

NAD_G304 – Reforço do treino de Segurança.

Indicador: Realização de três exercícios de evacuação.

Meta: 29 de dezembro.

4.1.2. 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 percebido 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 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.

4.1.2.1. DEPARTAMENTO DE DESENVOLVIMENTO E INOVAÇÃO (DDI)

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

Sensibilização, Formação e Treino (SFT)

Aumentar a literacia e a capacitação avançada dos cidadãos e dos trabalhadores é a finalidade para o desenvolvimento de atividades e projetos neste domínio.

No domínio da sensibilização, o Centro Internet Segura (CIS) dará continuidade ao trabalho desenvolvido pelo consórcio e pelo CNCS, assegurando a manutenção das iniciativas e atividades de sensibilização e treino, com particular destaque para a implementação do CIS - Cybersecurity LAB, uma solução que permitirá a disponibilização de um diretório de recursos orientados às mais variadas gerações. Estes recursos (numa lógica de *serious games*)¹ permitirão criar um laboratório de treino e aprendizagem suportado nos conceitos de “capture the flag”, onde os participantes terão acesso a um conjunto de desafios que possibilitarão a aquisição

¹ *Serious games* (dado que a literatura evidencia o seu potencial enquanto instrumento de apoio a uma aprendizagem rápida e eficaz), onde os participantes terão acesso a um conjunto de desafios que possibilitarão a aquisição de conhecimentos. Serious Games, também chamados de jogos baseados em computador ou jogos digitais tem cada vez mais chamado a atenção dos especialistas no seu potencial educativo (C. Conati, 2002). *Serious Game* é uma forma de jogos eletrónicos destinados a fins educacionais que promovam o ensino centrado no utilizador. (esta definição não é para ser integrada, claro). É só para se perceber do que estamos a falar.

de conhecimentos. Ainda neste domínio, os cursos e-learning continuarão a servir como instrumento central de sensibilização dos cidadãos em matéria de cibersegurança. Além dos quatro cursos já implementados e atualizados anualmente, prevê-se a criação de um novo curso e-learning intitulado Cidadão Ciberinclusivo, que visará tornar a cibersegurança acessível a todos os cidadãos, respondendo a necessidades especiais de pessoas com deficiência física, mental ou cognitiva. Também se prevê o desenvolvimento de conteúdos de boas práticas, nomeadamente as relacionadas com o de aplicações de mensagens instantâneas; boas práticas para a Internet of Things (IoT); e boas práticas contra o ransomware. Estas boas práticas pretendem contribuir para a sensibilização dos cidadãos em geral.

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

No âmbito do treino, em particular na identificação e captação de jovens talentos nacionais em cibersegurança, o Cybersecurity Challenge PT será o instrumento que permitirá capitalizar este objetivo. A criação de uma comunidade nacional de jovens com interesses em STEM (Ciências, Tecnologia, Engenharia e Matemática) em canais e redes próprias, dinâmica e ativa ao longo do ano com envolvimento de antigos participantes nesta competição, jovens estudantes, universidades, ensino secundário e sociedade civil será a forma de alavancar a notoriedade da atividade. O Exercício Nacional de Cibersegurança é outro dos instrumentos a implementar, promovendo o treino e a qualificação de entidades na área da cibersegurança para prevenção e reação a incidentes, e a formação de uma comunidade de conhecimento e de uma cultura de cibersegurança.

Conhecimento Situacional (CS)

De modo a informar as partes interessadas, produzir conhecimento situacional e suportar a definição de políticas públicas, o Observatório de Cibersegurança, através de uma visão multidisciplinar, sistematiza informação disponível ou promove a sua recolha nos domínios da Sociedade, Economia, Políticas Públicas, Ética e Direito, Riscos e Conflitos, bem como Inovação e Tecnologias Futuras. Neste sentido, no ano de 2023, manter-se-á a produção anual dos relatórios Riscos & Conflitos, Sociedade e dos Boletins. Pretende-se ainda produzir um Referencial de Transição Digital e Cibersegurança, os estudos Criptomoedas e Blockchain, Cibersegurança na Administração Pública e Ensino e Preparação de um Futuro Ciberseguro, bem como uma nova edição do relatório Ética & Direito. Estas serão pesquisas que contribuirão para a análise da realidade e para a tornar mais compreensível.

Em 2023, manter-se-ão as atividades recorrentes de controlo da execução do Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço 2019-2023, com momentos chave entre janeiro e março, com o controlo da execução entre abril e junho, com a revisão das medidas inscritas para 2023 e eventual término. A par desta atividade será prestado o apoio na preparação da próxima Estratégia Nacional na área da cibersegurança, ainda em análise no Conselho Superior de Segurança do Ciberespaço.

Comunicação e Imagem (C&I)

No que diz respeito à Comunicação externa, continuar-se-á a dar prioridade ao desenvolvimento de estratégias de comunicação que visem chegar o resultado dos projetos e atividades do CNCS a uma base cada vez mais alargada de diferentes comunidades e públicos. Uma estratégia de comunicação multiplataforma, incluindo redes sociais e parcerias com meios de comunicação especializados e generalistas e com associações

de classe profissionais e industriais, será o meio para atingir este fim. Serão desenvolvidas campanhas de boas práticas e de contexto atual, que terão como meios de comunicação preferenciais a televisão, a rádio, a publicidade institucional através das principais Câmaras Municipais, das Redes de Transportes Públicos, da rede SIBS, e ainda, recorrendo a alguns *influencers*. Dar-se-á, em 2023, especial enfoque à comunicação dirigida aos gestores e decisores das empresas/entidades através de uma abordagem conjunta de meios especializados, comunidades intermunicipais e de associações empresariais.

No âmbito do “Comunicar Cibersegurança – o podcast do CNCS”, um espaço de discussão sobre temas que pretendem servir para a promoção e reflexão das matérias de interesse relacionadas com a Cibersegurança, continuar-se-á a desenvolver as próximas edições, tendo em vista as publicações periódicas que o programa exige.

No âmbito dos eventos iremos realizar seis grandes eventos, entre outros de menor dimensão. A C-DAYS, que voltará a reunir líderes empresariais e do setor público, especialistas e académicos para discutir experiências e caminhos a adotar no crescimento da maturidade em Cibersegurança, no Porto, e na Madeira e Açores através de coorganização com organismos regionais. O Fórum da Cibersegurança na Administração Pública, que reunirá entidades que contribuem para o Plano de Ação da Estratégia Nacional de Segurança do Ciberespaço, membros dos organismos TIC (CTIC) e representantes dos Governos Regionais da Madeira e Açores para discutir estrategicamente linhas de ação que apoiem e dinamizem o reforço da cibersegurança na Administração Pública. O Dia da Internet mais Segura, dinamizado em estreita colaboração com o consórcio Centro Internet Segura (CIS), que reúne jovens, académicos e especialistas com vista a aumentar a sensibilização para a segurança online das crianças e jovens. E o Exercício Nacional de Cibersegurança cujo objetivo é promover o treino e a qualificação de entidades na área da cibersegurança para prevenção e reação a incidentes de cibersegurança, e a formação de uma comunidade de conhecimento e de uma cultura de cibersegurança.

Paralelamente, haverá lugar à dinamização de sessões temáticas de Cibertemas, tendo em vista a escolha de temas de interesse genérico, com o objetivo de ter um significativo alcance público e momentos de destaque mediático, tais como o European Cybersecurity Month e o Girls in ICT, cujo objetivo deste último é fomentar a igualdade de género na área da cibersegurança.

4.1.2.1.1. OBJETIVOS OPERACIONAIS

DDI_PI105 – Lançamento do C-Lab CIS.

Indicador: Lançamento do C-Lab CIS ao público em geral.

Meta: 31 de dezembro

DDI_PI106 – Formandos certificados pela C-Academy.

Indicador: Número de certificados emitidos.

Meta: 1400

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.1 – Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como submedida TD C19 i03.1.2- Academia de Cibersegurança, para concretização do objetivo, inscrito no contrato do PRR, como meta 19.7 Formação de especialistas em TI para reforçar as capacidades de cibersegurança e segurança da informação, visando formar 9 800 especialistas.

DDI_PI107 – Publicação de relatórios.

Indicador: Número de relatórios publicados.

Meta: 5

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.3 – Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação de Cibersegurança e da segurança da informação, identificada internamente, como submedida TD C19 i03.3.4- Observatório de cibersegurança, para concretização do objetivo, inscrito no contrato do PRR, como meta 1375 – Produção sistematizada e atualizada de indicadores de cibersegurança, visando publicar 16 relatórios.

4.1.2.2. DEPARTAMENTO DE CAPACITAÇÃO TÉCNICA (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, serviços e ferramentas desenvolvidas a pensar no crescimento e maturidade da Cibersegurança das organizações nacionais.

O DCTO apoia o desenvolvimento de capacidades nas organizações através da dinamização e reforço de ações de redes de colaboração e criação de sinergias, troca de experiências e envolvimento em projetos colaborativos. Adicionalmente, tem a seu cargo a produção de documentação de apoio às organizações, sob a forma de boas práticas, guias e recomendações técnicas, prestando também apoio na sua operacionalização.

Capacidades nas Organizações (CO)

Ao nível do desenvolvimento de capacidades nas organizações, será dada prioridade à operacionalização de alguns projetos colaborativos.

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

Também o polo de inovação digital C-HUB: Cybersecurity DIH (C-HUB), foi criado para fomentar a introdução da inovação e cibersegurança nos processos de transformação digital, com o intuito de apoiar as PMEs e entidades da Administração Pública no seu caminho para a Ciber-resiliência. Consistindo num consórcio de sete entidades e numa lógica de “Testar antes de investir”, o C-HUB fornecerá atividades de experimentação e demonstração, prototipagem, certificação e transferência de tecnologia em cibersegurança, assumindo-se deste modo como uma referência na implementação de processos de transformação digital. No ano de 2023, com a previsão de aprovação de candidatura a financiamento nacional, o C-HUB iniciará as suas atividades visando a prossecução da estratégia e objetivos previstos.

Na sequência da constituição do CNCS como Centro Nacional de Coordenação (CNC), no âmbito da rede de centros nacionais de coordenação para a cibersegurança no espaço europeu, e da sua articulação com a

Agência Nacional de Inovação (ANI) e Fundação para a Ciência e a Tecnologia (FCT), num modelo de responsabilidades partilhadas, através da criação de um consórcio entre estas entidades, interessa agora garantir a operacionalização do CNC e a prossecução das suas principais atribuições. Nesse sentido, caberá ao CNCS assegurar a coordenação e acompanhamento das ações tomadas no âmbito do consórcio; a comunicação entre o consórcio e o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Comissão; a gestão e execução das subvenções atribuídas ao CNC, de acordo com as decisões e estratégias definidas em conjunto pelos membros do consórcio.

Redes de Colaboração (RC)

No que diz respeito às redes de colaboração nas quais o CNCS se encontra envolvido, destaca-se a promoção das atividades de cooperação e troca de experiências no âmbito dos vários ISACs e a dinamização das primeiras atividades da Aliança para a Cibersegurança.

A criação e dinamização de Centros de Análise e Partilha de Informação (ISACs) serve o objetivo de fomentar o desenvolvimento de comunidades de parceiros no âmbito dos setores mais críticos ou sensíveis. Através da promoção da confiança e debate entre pares, pretende-se estimular e acompanhar continuamente os ISACS já criados e, por outro lado, proporcionar a operacionalização dos ISACs setoriais das telecomunicações, saúde e banca; e dos ISACs regionais dos Açores e Municípios desta região autónoma. Adicionalmente, e numa perspetiva de garantir o necessário suporte técnico à dinamização e aproximação destas comunidades, será selecionada e disponibilizada uma plataforma de comunicação aos vários ISACs nacionais.

Ainda no âmbito da dinamização das redes de colaboração, a Aliança para a Cibersegurança desenvolverá as suas primeiras atividades no ano de 2023. Conta atualmente com doze membros que irão desenvolver várias atividades de partilha de conhecimento e capacitação para pequenas e médias empresas.

Guias e Normativos Técnicos (GNT)

No âmbito da disponibilização do Selo Digital de Cibersegurança e da importância que lhe é reconhecida como instrumento de capacitação em cibersegurança para organizações de pequena e média dimensão, será produzido e disponibilizado um guia para melhor compreensão e apoio à implementação dos seus requisitos. Adicionalmente, e com o objetivo de potenciar este instrumento de capacitação, será desenvolvido um estudo comparativo com outros mecanismos semelhantes e uma proposta de possíveis cenários para a sua evolução.

De modo a assegurar o acompanhamento da evolução dos standards e boas práticas de cibersegurança, sem esquecer outros temas e tendências atuais de maior relevo (como por exemplo, a importância da utilização de mecanismos de múltiplo fator de autenticação, arquiteturas zero-trust, etc.), será produzida e publicada documentação sob a forma de boas práticas, guias e recomendações técnicas.

4.1.2.2.1. OBJETIVOS OPERACIONAIS

DCTO_PI108 – Contratualização dos Centros de Competência (Nº de contratualizações) (**Objetivo operacional do QUAR 2023 – Relevante**).

Indicador: Número de contratos formalizados.

Meta: 3.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.1 – Reforçar a capacitação em cibersegurança e segurança da informação, identificada internamente, como

submedida TD C19 i03.1.1- Rede de Centros de Competência, para concretização do objetivo, inscrito no contrato do PRR, como meta 1358 – Criar uma rede centros de competência em Cibersegurança, visando o desenvolvimento de soluções inovadoras em Cibersegurança para PME e estruturas públicas locais e regionais, visando a instalação de 7 centros de competência.

DCTO_PI109 – Criação das comissões de Acompanhamento e de Ética do C-Hub.

Indicador: Ata de tomada de posse.

Meta: 30 de junho.

DCTO_P118 – Operacionalização da plataforma de comunicações.

Indicador: Registos de comunicação intra ISAC (centros de análise e partilha de informação) na plataforma de comunicações.

Meta: 31 de outubro.

4.1.2.3. DEPARTAMENTO DE OPERAÇÕES (DO)

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

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

Neste âmbito são assegurados os seguintes serviços:

Gestão e coordenação a resposta a incidentes de cibersegurança no ciberespaço de interesse nacional (GCI);

Deteção e prevenção de incidentes de cibersegurança no ciberespaço de interesse nacional (DPI);

Produção do Quadro Situacional da Cibersegurança Nacional (QS);

Gestão e Coordenação de Incidentes (GCI)

No âmbito da gestão dos incidentes o plano de atividade 2023 incluirá uma etapa de sistematização de procedimentos operacionais. É exetável que o número de incidentes reportados ao CERT.pt durante o ano de 2023 venha a subir de forma considerável. Para facilitar o processamento desses incidentes pretende-se, por via da adoção de procedimentos operacionais standardizados, reduzir o tempo despendido com cada um deles potenciando a disponibilidade da equipa para executar outras tarefas igualmente relevantes.

A atividade primordial do CERT.pt terá durante 2023 uma melhoria na sua capacidade de resposta a incidentes. Para tal pretende-se evoluir hardware e software dedicado a esta tarefa, procurando soluções que permitam a prestação de um melhor serviço à comunidade servida pela instituição.

A recolha de indicadores de comprometimento em redes e sistemas afetados por ataques informáticos é um importante vetor na obtenção de dados únicos que permitam efetuar ações preventivas em alvos

semelhantes. Pretende-se capacitar o CERT.pt de meios de recolha, processamento e armazenamento de dados forenses avançados.

A comunicação, na vertente que respeita à resposta a incidentes, é um aspeto de primordial importância para a informação devida ao público em geral, gerando variações positivas no sentimento de cibersegurança geral. Ao mesmo tempo, é fulcral para o CERT.pt evitar, através de uma comunicação frugal, mas assertiva, a formação de tendências de opinião erradas, geradas a partir de discussões e *posts* na *web*, que podem gerar cenários díspares da realidade verificada.

Deteção e Prevenção de Incidentes (DPI)

A memória, em cibersegurança, é de extrema relevância para a inferência de ações maliciosas futuras. De facto, a análise de casos passados anonimizados permite a formação de previsões baseadas na repetição de técnicas e procedimentos utilizados em casos anteriores. A criação de repositórios de dados enviados ao CERT é, por isso, uma tarefa a executar durante 2023.

Quadro Situacional (QS)

No âmbito da produção de um Quadro Situacional da Cibersegurança Nacional, o PANORAMA incrementa a visibilidade sobre o conjunto de entidades de interesse que concorrem para o cibersegurança nacional. Para este objetivo dar-se-á continuidade à caracterização das atividades de organismos (públicos ou privados), privilegiando entidades com quem o CNCS já mantém acordos de cooperação firmados ou que sejam Operadores de Serviços Essenciais (OSE).

A ferramenta que permite ao CNCS ter visão global do estado do ciberespaço nacional, num qualquer momento presente, continuará a ser desenvolvida durante 2023.

4.1.2.3.1. OBJETIVOS OPERACIONAIS

DO_PI110 – Implementação de piloto de equipa de intervenção.

Indicador: Intervenção no primeiro caso.

Meta: 30 de junho.

DO_P119 – Implementação do plano comunicacional no procedimento operacional.

Indicador: Plano implementado.

Meta: 31 de outubro.

DO_PI111 – Caracterização de Entidades Operadoras de Serviços Essenciais e administração Pública (**Objetivo operacional do QUAR 2023 – Relevante**).

Indicador Número de entidades caracterizadas.

Meta: 40.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.3 – Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação de Cibersegurança e da segurança da informação, identificada internamente, como submedida TD C19 i03.3.3- PANORAMA, inscrito no contrato do PRR, como meta 19.9 – Implementação de mecanismos da manutenção

evolutiva PANORAMA; Aquisição de serviços e equipamento com vista à ligação segura de novas entidades; Aquisição de *feeds* de *cyber intelligence*; Reestruturação da sala de situação para responder ao crescimento do CERT.PT e a desafios emergentes; Produção de relatórios de análise mensais para as entidades participantes (operadores de serviços essenciais e organismos TIC da administração pública, visando a caracterização de 27 e 40 entidades (OSE e AP), respetivamente.

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

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

O Departamento de Regulação, Supervisão e Certificação (DRSC) contempla ainda as áreas referentes às funções de Autoridade Nacional de Certificação da Cibersegurança decorrentes do Regulamento UE 2019/881 e do Decreto-Lei n.º 65/2021, de 30 de julho, que atribui ao CNCS essa competência.

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

O DRSC procede ainda ao planeamento e condução de exercícios de cibersegurança, assegura as funções de CISO do GNS / CNCS e garante a prestação de uma gama de outras atividades permanentes, como a representação em fórum internacionais, o apoio à Tutela, a cooperação nacional e internacional e a participação em eventos ad hoc.

Regulação e Supervisão (R&S)

Em 2023 serão produzidos normativos nos termos do n.º 1 do artigo 18.º do Decreto-Lei n.º 65/2021, de 30 de julho, adaptados aos diversos setores de atividade abrangidos pela Diretiva NIS e pelo Regime Jurídico de Segurança do Ciberespaço, nas áreas da saúde e da energia.

Serão realizadas atividades de preparação da Autoridade Nacional da Cibersegurança para o exercício das competências e responsabilidades adquiridas pela publicação da revisão da Diretiva da Segurança das Redes e da Informação (NIS 2) e outros normativos, como o Cyber Resilience Act e a Diretiva CER, entre outros. Para esta atividade, irá ser conduzido um estudo de impacto dos referidos normativos no RJSC, incluindo a identificação de necessidades de atualização e aperfeiçoamento do RJSC, de que resultará proposta para as necessárias medidas adaptativas, com vista à transposição da NIS2 para o ordenamento jurídico nacional.

Continuação da participação nacional no processo europeu de cooperação em matéria de cibersegurança em sede do Grupo de Cooperação da Diretiva da Segurança das Redes e da Informação (NIS Cooperation Group), através da dinamização e liderança de iniciativas no contexto dos Work Streams alusivos ao 5G, prestadores de serviços digitais e infraestruturas digitais, e da liderança do WS12 da Saúde. Em 2023, perspetiva-se, pela

Comissão e restantes Estados-Membros e em função das alterações decorrentes da NIS2, a priorização de work streams horizontais, como o do Work Stream on cybersecurity requirements and vulnerability management, e o DRSC irá acompanhar essa dinâmica.

O DRSC irá ainda promover a realização em Portugal de uma reunião presencial do WS12 da Saúde, que poderá marcar o culminar do ciclo inicial de atividade deste Work Stream.

De igual forma, proceder-se-á ao desenho e implementação de procedimentos para fiscalizar, auditar, aplicar sanções e coimas, e de recurso para contencioso, para as entidades abrangidas pelo Regime Jurídico de Segurança do Ciberespaço, priorizando e acompanhando a evolução dos trabalhos da regulamentação terciária da Lei 46/2018, de 13 de agosto, incluindo sobre procedimentos de supervisão partilhada, sempre que adequados e exequíveis, conjuntamente com as entidades setoriais com poderes de regulação e de supervisão.

O DRSC irá ainda, em cumprimento do contrato do PRR, promover a formação e a capacitação de auditores especializados, para constituição de uma bolsa de peritos qualificados para a execução de auditorias de cibersegurança.

Certificação (CTF)

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

As novas e importantes responsabilidades do CNCS enquanto Autoridade Nacional de Certificação da Cibersegurança junto da União Europeia implicam um trabalho rigoroso de preparação da organização para o exercício da supervisão e monitorização dos certificados e declarações de conformidade emitidos no contexto de esquemas europeus de certificação, do cumprimento das regras e obrigações incluídas em tais esquemas pelas entidades emitentes de declarações de conformidade e por organismos de certificação nacionais; e para a emissão de certificados UE de nível “Elevado”, sempre que determinado esquema europeu de certificação preveja tal nível.

Ao DRSC, por via da segregação que deverá ocorrer, por requisito legal inserido no Regulamento UE 2019/881, no seio da Autoridade Nacional de Certificação da Cibersegurança entre a área de supervisão da certificação UE e a área de certificação / emissão de certificados UE, caberá a condução das atividades de supervisão da certificação UE. Assim, o DRSC terá como linha de ação, neste domínio, a operacionalização das atividades de supervisão da certificação pela Autoridade Nacional de Certificação da Cibersegurança. Esta linha de ação poderá explorar a existência de sinergias com a atividade de supervisão do RJSC (DRSC#1) ou, pelo menos, a prevenção de ineficiências e duplicações supérfluas.

Publicado o Esquema de certificação do Quadro Nacional de Referência para a Cibersegurança (EC QNRCS), importa imprimir-lhe energia e dedicar-lhe recursos suficientes para ganhar tração e implantar-se no contexto nacional, isto é, até que seja adotado por um número mínimo de organismos certificadores e entidades certificadas, que lhe confirmem massa crítica e reputação para o seu desenvolvimento autónomo. O DRSC irá promover a divulgação e a adoção do esquema, através de iniciativas de informação, sensibilização e divulgação, como a produção de referenciais de suporte e conteúdos informativos, e de apoio a entidades interessadas ou candidatas. Ainda neste âmbito, o DRSC irá ainda, em cumprimento do contrato do PRR, facilitar a acreditação de organismos para o exercício de atividades de certificação no contexto do Esquema

de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança, e ainda divulgar e promover, através de ações direcionadas, a candidatura de organismos da Administração Pública à certificação neste Esquema. Após a entrada em operação do Esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança e tendo, já desde há algum tempo, sido identificada a necessidade de elaboração de um catálogo de prestadores nacionais de serviços de cibersegurança confiáveis e de qualidade, o DRSC irá promover, como segundo esquema do Quadro Nacional de Certificação da Cibersegurança, a elaboração de um esquema de certificação de empresas de serviços de cibersegurança.

A certificação neste novo esquema procurará responder assim a necessidades internas, de constituição de um corpo de empresas e prestadores de serviços de qualidade no ramo da cibersegurança que atendam à procura destes serviços, inclusive para cumprimento de requisitos legais, e a necessidades externas, elevando a reputação das empresas nacionais e permitindo a sua introdução pelo CNCS ou outros agentes, com credibilidade, no mercado europeu da cibersegurança.

Planeamento de emergência e de coordenação de crises do ciberespaço (PE CCC)

Atividade em prol do planeamento de emergência e de coordenação de crises do ciberespaço, integrando e articulando componentes como a ativação da Comissão de Planeamento de Emergência da Cibersegurança criada no contexto do Sistema Nacional de Planeamento Civil de Emergência, instituído pelo Decreto-Lei n.º 43/2020, de 21 de Julho, o plano nacional de emergência de cibersegurança e o procedimento para definição de nível de alerta nacional para o ciberespaço, e os requisitos a nível da rede CyCLONe para criação de estrutura nacional de coordenação de crises e respetivos procedimentos-base.

4.1.2.4.1. OBJETIVOS OPERACIONAIS

DRSC_P120 – Formação de auditores especializados.

Indicador Número de Certificados de formação.

Meta: 8.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.3 – Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação de Cibersegurança e da segurança da informação, identificada internamente, como submedida TD C19 i03.3.1-Supervisão, inscrito no contrato do PRR, como meta 1371 – Formar e capacitar auditores especializados, visando identificar 12 auditores especializados.

DRSC_P121 – Normativo setorial - OSE Energia - entrega de proposta final.

Indicador Entrega de proposta final de normativo setorial para validação pela Tutela.

Meta: 31 de junho.

DRSC_P122 – Acreditação de organismos de certificação da conformidade com o QNRCS na AP.

Indicador Número de organismos acreditados.

Meta: 2.

Nota: A concretização deste objetivo será suportada pelo investimento PRR, através da medida TD C19 i03.3 – Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação de Cibersegurança e da segurança da informação, identificada internamente, como submedida TD C19 i03.3.2-

Certificação em Cibersegurança, inscrito no contrato do PRR, como meta 1372 – Acreditação faseada de 2 organismos de avaliação de conformidade para as novas competências decorrentes da evolução do quadro normativo nacional e internacional da cibersegurança, visando capacitar 2 organismos acreditados.

4.1.2.5. DEPARTAMENTO DE SERVIÇOS TÉCNICOS(DST)

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

Gestão de Sistemas e Infraestruturas (GSI)

A área de Gestão de Sistemas e Infraestruturas assegura a disponibilização, gestão e manutenção dos sistemas de suporte ao CERT.PT e à Rede Corporativa do GNS/CNCS. No seu âmbito, são também desenvolvidas atividades regulares de apoio à manutenção da Infraestrutura, de onde se destaca a renovação do parque de servidores, a atualização da infraestrutura de virtualização e diversas operações de manutenção e atualização de software. Nesse sentido, em 2023 será feita uma aposta na implementação de alguns serviços estruturantes tanto da atividade do DST como do próprio CNCS como um todo, nomeadamente a criação de um sistema de gestão de servidores Linux, a implementação de um sistema de gestão de acessos privilegiados e a criação de um sistema de gestão de identidade e acesso centralizado.

No âmbito da atualização de serviços relevantes para a disseminação de informação e comunicação, será efetuada a atualização do servidor de listas de distribuição de correio eletrónico, para uma versão mais recente.

Apoio ao utilizador (AU)

No que diz respeito à área de Apoio ao Utilizador, e para além das tarefas recorrentes de intervenção ao nível dos postos de trabalho, será mantida a aposta na renovação dos equipamentos afetos aos utilizadores, sempre que tal se justifique. Na sequência da necessidade de adaptação a um modelo de trabalho híbrido, e concretizada a autonomização do CNCS relativamente à sua infraestrutura de comunicações VoIP, será implementada uma solução que permita emular o telefone IP do utilizador no posto de trabalho e, desse modo, facilitar a comunicação externa e interna no âmbito da transição entre trabalho remoto e presencial.

Security Operations Center (SOC)

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

À imagem do que foi desenvolvido no âmbito do CERT.PT, será disponibilizada uma ferramenta centralizada para a recolha, armazenamento e consulta de registos (logs) gerados pelos recursos afetos à Rede Corporativa do GNS/CNCS, o que permitirá atingir um maior grau de visibilidade sobre a atividade dos sistemas. Para esta visibilidade também contribuirá um novo sistema de proxy de acesso à Internet, a renovação do sistema de resolução de nomes interno e a recolha de netflows internos.

A estas atividades, e na sequência do trabalho desenvolvido em 2022, acrescenta-se a operacionalização da plataforma de gestão de incidentes de segurança, ferramenta essencial no registo, gestão e controlo dos incidentes de segurança geridos pelo SOC.

4.1.2.5.1. OBJETIVOS OPERACIONAIS

DST_P123 – Implementação de sistema de gestão de acessos privilegiados.

Indicador: Entrada em produção.

Meta: 30 de dezembro.

DST_P124 – Centralização de logs de toda a rede.

Indicador: Entrada em produção.

Meta: 30 de junho.

DST_G204 – Construção de Plano de continuidade de negócio.

Indicador: Aprovação da documentação de suporte e restantes evidências técnicas.

Meta: 31 de dezembro.

5. RECURSOS HUMANOS

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

Em 30 de dezembro de 2020 o GNS dispunha de 91 postos de trabalho ocupados, sendo 46,15% de pessoal militar, 12,08% proveniente das forças de segurança e 41,77% pessoal civil.

O recrutamento de elementos para o CNCS e a entrada de pessoal das Forças Armadas e Forças de Segurança, permitiu preencher diversos postos de trabalho, pelo que no final de 2021 existiam 100 postos de trabalho preenchidos no GNS/CNCS.

Em 2022 prosseguiu-se o esforço de recrutamento de pessoal, tendo-se preenchido 113 postos de trabalho, de modo que o GNS/CNCS garantisse as suas atribuições.

Em 2023 irá prosseguir-se o esforço de recrutamento de pessoal, afigurando-se como necessário, para que o GNS/CNCS assegure as suas atribuições, o preenchimento de 122 postos de trabalho.

O quadro seguinte projeta, de acordo com o Mapa de Pessoal aprovado para 2023 (ANEXO E), os quantitativos globais de pessoal necessário para o desempenho das atribuições do GNS e do CNCS.

5.1. RECURSOS HUMANOS

Proveniência/natureza	Quantitativos	
	GNS	CNCS
Forças Armadas (militares)	64	0
Forças de Segurança (GNR/PSP)	9	0
Civis	9	40
Sub Totais	82	40
TOTAL	122	

5.1.1. MAPA DISCRIMINATIVO

Categoria/Qualificação	Quantitativos	
	GNS	CNCS
Dirigentes Superiores	1 Diretor Geral	
	1 Subdiretor Geral	1 subdiretor Geral
Oficiais das Forças Armadas	28	-
Sargentos das Forças Armadas	31	-
Praças das Forças Armadas	10	-
Agentes da PSP	3	-
Técnicos Superiores	1	-
Consultores Coordenadores	-	5
Consultores	3	9
Técnicos		24
Assistentes Técnicos	3	1
Assistentes Operacionais	2	-
Sub Totais	82	40
TOTAL	122	

5.2. RECURSOS FINANCEIROS

5.2.1. VALORES INSCRITOS/PROPOSTOS NO OE-2023

Funcionamento	FF 311	Agrupamento 01 - Pessoal	505.552,00 €
	Atividade 231	Agrupamento 02 - Bens e Serviços	172.116,00 €
	GNS	Agrupamento 07 - Despesas Capital	0,00€
		<i>Subtotal 231</i>	<i>677.668,00€</i>
	FF 311	Agrupamento 01 - Pessoal	1 895 974,00 €
	Atividade 171	Agrupamento 02 - Bens e Serviços	653 378,00 €
	CNCS	Agrupamento 07 - Despesas Capital	166 200,00 €
		<i>Subtotal 171</i>	<i>2 715 552,00 €</i>
		Total FF 311	3 393 220,00 €
	FF 513	Agrupamento 01 - Pessoal	25.000,00 €
	Atividade 231	Agrupamento 02 - Bens e Serviços	837 000,00 €
	GNS	Agrupamento 06 - Reserva	35 000,00 €
		Agrupamento 07 - Despesas Capital	503 000,00 €
		Total FF 513	1 400 000,00 €
		Total FF 311 + FF513	4 793 220,00 €

Comparticipação Nacional

Programa	Medida	Funcional	Fonte de Financiamento	Classificação Económica		Proj	Proposta OE2023
10303 - PROJETO CEF/TELECOM 1							
2	1	1011	357	D.07.01.07.A0.C0	OUTROS	10303	1 €
9888 - PROJETO DOGANA							
2	1	1011	357	D.02.02.20.A0.A0	DESENVOLVIMENTO DE SOFTWARE	9888	1 €
11103 - PROJETO CEF/TELECOM 2							
2	1	1011	357	D.07.01.07.A0.C0	OUTROS	11103	1 €
11570 - PROJETO PETRUS							
2	1	1011	357	D.02.02.20.00.00	OUTROS TRABALHOS ESPECIALIZADOS	11570	1 €
11575 - PROJETO PT SIC VI							
2	1	1011	357	D.02.02.20.E0.00	OUTROS	11575	1 €
12650 - PROJETO PT SIC VII							
2	1	1011	357	D.02.02.20.E0.00	Outros trabalhos especializados - Outros	12650	200 436 €
2	1	1011	357	D.07.01.07.A0.C0	Equipamento de informática - Outros	12650	3 500 €
11317 - PROJETO INTELIGÊNCIA ARTIFICIAL							
2	1	1011	351	D.02.02.20.A0.C0	OUTROS	11317	1 €
11567 - PROJETO CRESO							
2	84	1011	351	D.07.01.07.A0.C0	OUTROS	11567	1 €
							203 943,00€

Comparticipação Europeia

Programa	Medida	Funcional	Fonte de Financiamento	Classificação Económica	Proj	Proposta OE2023
10303 - PROJETO CEF/TELECOM 1						
2	1	1011	482	D.07.01.07.A0.C0 OUTROS	10303	1 €
9888 - PROJETO DOGANA						
2	1	1011	482	D.02.02.20.A0.A0 DESENVOLVIMENTO DE SOFTWARE	9888	1 €
11103 - PROJETO CEF/TELECOM 2						
2	1	1011	482	D.07.01.07.A0.C0 OUTROS	11103	1 €
11570 - PROJETO PETRUS						
2	1	1011	482	D.02.02.20.00.00 OUTROS TRABALHOS ESPECIALIZADOS	11570	1 €
11575 - PROJETO PT SIC VI						
2	1	1011	482	D.02.02.20.E0.00 OUTROS	11575	1 €
12650 - PROJETO PT SIC VII						
2	1	1011	482	D.02.02.20.E0.00 Outros trabalhos especializados - Outros	12650	200 436 €
2	1	1011	482	D.07.01.07.A0.C0 Equipamento de informática - Outros	12650	3 500 €
11317 - PROJETO INTELIGÊNCIA ARTIFICIAL						
2	1	1011	414	D.02.02.20.A0.C0 OUTROS	11317	1 €
11567 - PROJETO CRESO						
2	84	1011	414	D.07.01.07.A0.C0 OUTROS	11567	1 €
						203 943,00€

PRR

TD-C19-i03 - 12402 - Reforçar a capacitação em cibersegurança e segurança da informação									
2	102	483	D.02.02.09.A0.00	ACESSOS A INTERNET		12402			12 300 €
2	102	483	D.02.02.15. B0.00	OUTROS		12402			295 200 €
2	102	483	D.02.02.16.00.00	SEMINÁRIOS, EXPOSIÇÕES E SIMILARES		12402			162 975 €
2	102	483	D.02.02.20. E0.00	OUTROS		12402			2 268 735 €
2	102	483	D.07.01.07. A0.C0	OUTROS		12402			235 176 €
2	102	483	D.07.01.08. A0. B0	OUTROS		12402			10 824 €
TD-C19-i03 - 12410 - Incrementar a Segurança na Gestão do Ciclo de Vida da Informação									
2	102	483	D.02.02.14. D0.00	OUTROS		12410			61 500 €
2	102	483	D.02.02.15. B0.00	OUTROS		12410			55 350 €
2	102	483	D.02.02.20. E0.00	OUTROS		12410			455 100 €
2	102	483	D.07.01.03. A0. B0	CONSERVAÇÃO OU REPARAÇÃO		12410			61 500 €
2	102	483	D.07.01.07. A0.C0	OUTROS		12410			455 100 €
2	102	483	D.07.01.08. A0.B0	OUTROS		12410			270 600 €
2	102	483	D.07.01.09. A0. B0	OUTROS		12410			61 500 €
2	102	483	D.07.01.10. A0.B0	OUTROS		12410			492 000 €
TD-C19-i03 - 12425 - Implementar o quadro nacional de cibersegurança e transformar o atual modelo de coordenação da cibersegurança e da segurança da informação									
2	102	483	D.02.02.09.A0.00	ACESSOS A INTERNET		12425			2 460 €
2	102	483	D.02.02.14. D0.00	OUTROS		12425			200 490 €
2	102	483	D.02.02.15. B0.00	OUTROS		12425			307 500 €
2	102	483	D.02.02.20. E0.00	OUTROS		12425			879 450 €
2	102	483	D.07.01.03. A0.B0	OUTROS		12425			221 400 €
2	102	483	D.07.01.07. A0.C0	OUTROS		12425			1 476 000 €
2	102	483	D.07.01.08. A0.B0	OUTROS		12425			971 700 €

TD-C19-i03 - Projeto 4 - Criar as condições físicas e tecnológicas para a implementação e operacionalização do novo modelo de coordenação da cibersegurança e da segurança da informação						
2	102	483	D.02.02.14.D0.00	OUTROS	12433	49 200 €
2	102	483	D.07.01.03.A0.B0	OUTROS	12433	4 920 000 €
TD-C16-i03 - 12433 - Catalisação da Transição Digital das Empresas						
2	102	483	D.02.02.20.E0.00	OUTROS	12653	369 000 €
						14 295 060,00€

6. 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-se 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, em anexo F, 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 despendido com a formação dos recursos humanos do GNS/CNCS é, aproximadamente, de 335.000,00€, sendo cerca de 215.000,00 resultante do PRR, sendo o restante valor, cerca de 120.000€, suportado pelo orçamento de estado 2023.

O montante previsto despendido com a formação dos recursos humanos do GNS/CNCS é, aproximadamente, de 397.000,00€, sendo cerca de 275.000,00 resultante do PRR, sendo o restante valor, cerca de 122.000€, suportado pelo orçamento de estado 2023.

7. 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 2023, o GNS/CNCS propõe-se consolidar, efetuando melhorias e implementando novas funcionalidades, que se revelem necessárias ao funcionamento do sistema de Credenciações de Segurança Online (CRESO), a fim de facilitar a requisição de serviços pelos utentes, e dar continuidade às seguintes atividades:

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

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

8. PUBLICIDADE INSTITUCIONAL

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

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

Lisboa 10 de fevereiro de 2023

O DIRETOR-GERAL
António José
Gameiro
Marques
António José Gameiro Marques
CALM

Digitally signed by
António José
Gameiro Marques
Date: 2023.05.22
09:52:09 +01'00'

Anexos:

- Anexo A – Mapa estratégico
- Anexo B – Perspetiva Genética
- Anexo C – Perspetiva de Processos
- Anexo D – Perspetiva dos Públicos de Interesse
- Anexo E – Objetivos Estratégicos e Operacionais
- Anexo F – Mapa de Pessoal - 2023
- Anexo G – Plano de Formação - 2023
- Anexo H – QUAR - 2023

ANEXOS

PÁGINA DEIXADA EM BRANCO

ANEXO A

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

MAPA ESTRATÉGICO

PÁGINA DEIXADA EM BRANCO

Mapa Estratégico

Visão

Contribuir para um Portugal mais seguro, através de um comportamento confiável, preventivo, em rede e inovador

Missão

Cumprir a missão com EFICÁCIA

M.1 Modernizar e Consolidar tempestivamente as capacidades do GNS e do CNCS, afim de contribuir para o incremento da segurança de Portugal

Públicos de Interesse

Empregar as capacidades para melhor cumprir a missão

PI.1 Capacitar os públicos de interesse para os desafios da sociedade do conhecimento

PI.2 Gerir o ciclo de vida da ENSC 2019-2023

PI.3 Robustecer a capacidade de conhecimento do ciberespaço relevante e de proteção da sociedade

PI.4 Consolidar a moldura legislativa que enquadra o cumprimento da missão

Processos

Prosseguir com a otimização processual e organizacional

P.1 Modernizar a forma como prestamos o serviço e somos percecionados pelos nossos públicos de interesse

P.2 Analisar e incorporar novas realidades, novos conceitos e tecnologias emergentes com impacto na missão

P.3 Capacitar para fazer face aos novos desafios

Genética

Prosseguir com a edificação equilibrada de capacidades, incluindo a respetiva sustentação

G.1 Investir na formação e no bem-estar dos colaboradores

G.2 Capacitar para a gestão da informação como potenciador da estratégia

G.3 Robustecer a capacidade e a resiliência organizacional

Valores

Lealdade Confiabilidade Honestidade Rigor Honra Integridade

PÁGINA DEIXADA EM BRANCO

ANEXO B

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

PERSPETIVA GENÉTICA

PÁGINA DEIXADA EM BRANCO

Perspetiva genética

Prosseguir com a edificação equilibrada de capacidades, incluindo a respetiva sustentação



G.1 - Investir na formação e no bem-estar dos colaboradores

Promover a formação dos colaboradores pertinente e atempada

Fomentar a comunicação transversal para incremento da coesão organizacional

Acautelar a Higiene, Segurança e Saúde no trabalho

Promover a partilha de conhecimento

Promover o *Team building*
Tornar as infraestruturas mais amigas do ambiente



G.2 - Capacitar para a gestão da informação como potenciador da estratégia

Criar as condições para que a informação se transforme em conhecimento acionável através de:

(1) Criação de *Dashboards* de apoio à decisão (FIN, RH, Gestão da Execução da Estratégia)

(2) Prossecução da desmaterialização de processos

(3) Criação de áreas colaborativas



G.3 - Robustecer a capacidade e a resiliência organizacional

Consolidar "Continuidade de Negócio" (BC) e Plano de Recuperação de Atividades (DR)

Atualizar Plano de Mitigação de Risco

Reforçar a capacidade interna, designadamente em *Compliance*, Gestão de Projetos e Gestão ADM/FIN

Promover condições de retenção e estabilidade nos quadros de pessoal

PÁGINA DEIXADA EM BRANCO

ANEXO C

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

PERSPETIVA DE PROCESSOS

PÁGINA DEIXADA EM BRANCO

Perspetiva de Processos

Prosseguir com a otimização processual e organizacional

P.1 Modernizar a forma como somos percebidos e prestamos os serviços aos nossos Públicos de Interesse

Prosseguir com projetos em curso:

- CRM OSE (CNCS)
- Portal CNCS 2.0
- SCRIPTO (GNS)
- Consolidação CRESO (GNS)
- eSEIF (GNS)

Incremento da rede de parceiros (Setor público, Universidade e Politécnicos, Rede de CISOS, Rede de Prestadores de Serviços de confiança, Associações empresariais)

Inovar na forma de dar formação, investindo numa lógica de proximidade

P.2 – Analisar e incorporar novas realidades, novos conceitos e tecnologias emergentes com impacto na missão

Conceito de influências, ameaças e conflitos híbridos

Tecnologias de comunicação e computação quânticas

Impacto do 5G e do IOT

Comunicação segura via SAT (GALILEO)

Blockchain e segurança

...

P.3 Capacitar para fazer face a novos desafios

Reorg. Interna do CNCS

Reorg. Interna do GNS

Reorg. Estrutural

Melhoria dos processos de planeamento e de monitorização do desempenho organizacional

Apoiar a preparação das entidades nacionais atinentes no ciclo da Presidência PT do CE (1TR21)

Incrementar recurso a fundos comunitários

PÁGINA DEIXADA EM BRANCO

ANEXO D

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

PERSPETIVA DOS PUBLICOS DE INTERESSE

PÁGINA DEIXADA EM BRANCO

Perspetiva dos Públicos de Interesse

Empregar as capacidades para melhor cumprir a missão

PI.1 Capacitar os públicos de interesse para os desafios da sociedade do conhecimento

Aumentar o alcance dos instrumentos do CNCS para sensibilização e capacitação em cibersegurança de cidadãos e empresas

Aumentar o conhecimento das entidades dos setores público e privado quanto aos requisitos para a tramitação da Informação Classificada e da utilização dos meios de Identificação Eletrónica

PI.2 - Gerir o ciclo de vida da ENSC 2019 - 2023

Coordenar processo e alinhar objetivos
Fomentar a partilha de conhecimento e de boas práticas
Analisar novas realidades quanto ao potencial impacto na ENSC
Coordenar a execução do Plano de Ação
Coordenar processo de revisão

PI.3 - Robustecer a capacidade de conhecimento e de proteção da sociedade e do ciberespaço relevante

Melhorar a qualidade e o alcance do serviço de reação a ciberincidentes do CERT.PT (WEBCHECK, CyberCheck)
Ligar novas entidades ao PANORAMA
Continuar a edificar o Observatório de Cibersegurança
Consolidar a articulação ao nível operacional (G4)

PI.4 - Consolidar a moldura legislativa que enquadra o cumprimento da missão.

Prosseguir com a Reg. da Lei 46/2018 de 13 de agosto e atualizá-la em conformidade
Concluir processo do Diploma sobre Segurança da IC
Concluir processo de Diploma de adaptação do reg. eIDAS
Diplomas decorrentes do Cybersecurity ACT

PÁGINA DEIXADA EM BRANCO

ANEXO E

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

OBJETIVOS ESTRATÉGICOS E OPERACIONAIS

PÁGINA DEIXADA EM BRANCO

PA 2023 GNS/CNCS - OBJETIVOS ESTRATÉGICOS E OPERACIONAIS

Objetivos operacionais										OBS.
Enunciado	Linhas de ação	Código	Projecto	Indicador				EPR Orçânlco	EPR Nominal	
				Objetivo PRR	Meta PRR	Fonte de Financiamento	Tipologia	Meta 2023		
Públicos de Interesse	PI	DF_PH101	Promover ganhos de eficiência no domínio da formação interna e externa (% índice de satisfação)	N/A	N/A	OE	Índice de satisfação médio (em %) dos formandos que frequentaram ações de formação ministrada pelo GNS	85%	Objetivo operacional do QUAR 2023 – Relevante	
		GLCC_PH102	Otimizar a utilização das instalações do "Sub-Registo as a Service"	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.3-Sub-Registo as a Service	1366	PRR	Condução das melhorias nas infraestruturas do "Sub-Registo as a service"	30 de julho	Objetivo operacional do QUAR 2023 – Relevante	
		IRC_PH103	Implementação do "Disaster Recovery"	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.2 – Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada)	1365	PRR	Initial Operability Capability (IOC)	31 de outubro		
		IRC_PH104	Atualização de funcionalidades na Gestão Documental	N/A	N/A	OE	Data para Interoperabilidade da gestão documental com outros Organismos Públicos	31 de agosto		
		DOL_PH105	Lançamento do C-Lab CIS	N/A	N/A	OE	Lançamento do C-Lab CIS ao público em geral	31 de dezembro		
		DOL_PH106	Formandos certificados pela C-Academy	Medida TD C19.03.1-Reforçar a capacitação em cibersegurança e segurança da informação, submedida TD C19.03.1.2-Academia de Cibersegurança	15,7	PRR	Número de certificados emitidos	1400		
Públicos de Interesse	PI	DOL_PH107	Publicação de relatórios	Medida TD C19.03.3-Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação de Cibersegurança e da segurança da informação, submedida TD C19.03.3.4-Observatório de cibersegurança	1375	PRR	Número de relatórios publicados	5		
		DCTO_PH108	Contratualização dos Centros de Competência (Nº de contratualizações)	Medida TD C19.03.1-Reforçar a capacitação em cibersegurança e segurança da informação, submedida TD C19.03.1.1- Rede de Centros de Competência	1358	PRR	Número de contratos formalizados	3	Objetivo operacional do QUAR 2023 – Relevante	
		DCTO_PH109	Criação das comissões de Acompanhamento e de Ética do C-Hub	N/A	N/A	OE	Ata de tomada de posse	30 de junho		
		DO_PH110	Implementação de piloto de equipa de intervenção	N/A	N/A	OE	Intervenção no primeiro caso	30 de junho		
		DO_PH111	Caracterização de Entidades Operadoras de Serviços Essenciais e administração Pública	Medida TD C19.03.3-Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação de Cibersegurança e da segurança da informação, submedida TD C19.03.3.3-PANORAMA	1373/19,9	PRR	Número de entidades caracterizadas	40	Objetivo operacional do QUAR 2023 – Relevante	
		DF_PH101	Disponibilizar um curso sobre Segurança da Informação Classificada, num modelo de e-learning	Medida TD C19.03.1-Reforçar a capacitação em cibersegurança e segurança da informação, submedida TD C19.03.1.4- Qualificação de pessoas e organizações para poderem tratar informação	1362	PRR	Disponibilização do curso na plataforma e-learning	29 de dezembro		
Públicos		GLCC_PH102	Operacionalizar e certificar o Sistema de Segurança Eletrónica da Informação Classificada (eSEIF)	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.2- Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada)	1365	PRR	Operacionalizar software (SW) em órgãos de segurança	6 entidades		
						PRR	Processo de certificação do eSEIF	50% do processo de certificação		
		GLCC_PH103	Implementar novas funcionalidades e melhorias (eSEIF 2.0 e eSEIF Light)	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.2- Gestão da informação com necessidades especiais de segurança (SEIF, SCRIPTO Rede Classificada)	1365	PRR	Percentagem de desenvolvimento do novo SW que incluiu novas funcionalidades e melhorias	50%, do desenvolvimento		
							Data de aprovação do protocolo nacional para o financiamento do projeto entre as 4 entidades da administração central do Estado (GNS/IND/ENIG/FADEMOS)	1 de fevereiro		

PA 2023 GNS/CNCS - OBJETIVOS ESTRATÉGICOS E OPERACIONAIS

OBJETIVOS ESTRATÉGICOS				Objetivos operacionais					OBS.		
Enunciado	Linhas de ação	Código	Projeto	Objetivo PRR	Meta PRR	Fonte de Financiamento	Tipologia	Meta 2023		EPR Orçânica	EPR Nominal
Públicos	Incrementar a rede de parceiros (Setor público, Universidade e Politécnicos, Rede de CSOS, Rede de Prestadores de Serviços de confiança, Associações empresariais). Inovar na forma de formação, investindo numa lógica de proximidade.	GICC_P104	Participação no projeto DISCRETION, visando a disponibilização de uma solução Criptográfica Nacional a 150 de autoridades públicas até 2026	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.4-Capacidade Criptográfica Nacional	19,6	PRR	Desenho da rede Software Defined Network (SDN) com capacidade Quantum Key Distribution (QKD) e desenho da máquina de cifra com QKD (Work Package 5 (WP5) e Work Package 6 (WP6) e estudo da industrialização da máquina de cifra (WP6.3)	30 de setembro	GICC		
		GICC_P105	Operacionalização da implementação da plataforma de Gestão de Material Cripto (SCRIPTO)	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.2-Gestão da informação com necessidades especiais de segurança (SEIF SCRIPTO Rede Classificada)	1365	PRR	Data de aprovação de um Memorando pels 4 países participantes no projeto	28 de fevereiro			
		GICC_P106	Promover a melhoria dos processos através do desenvolvimento da máquina de cifra HSM-T2 para nova versão 2.1.	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, Submedida TD C19.03.2.4-Capacidade Criptográfica Nacional	19,8	PRR	Desenho de novo algoritmo de chaves internas mais robusto, ligação externa para programação e carregamento de chaves, bolido ZEROID, e revestimento de proteção para operações em ambientes desfavoráveis	2 de outubro	GICC		
		SDTL_P107	Implementar o Esquema Nacional de Certificação em Segurança Tecnológica de produtos e serviços habilitados a processar Informação Classificada	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.1-Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas	1364	PRR	Prazo para apresentação da proposta	30 de junho	SDTI		
		SDTL_P108	Robustecer a capacidade de contramedidas eletrônicas através do alargamento ao domínio acústico e desenvolvimento do manual de procedimentos em conjunto com o reforço da capacidade de acreditação e auditoria de sistemas de informação classificada	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.1-Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas	1364	PRR	Prazo para manifestação de necessidades das contramedidas eletrônicas para o domínio acústico	31 de março			
		SDTL_P109	Reforçar a capacidade de certificação de sistemas, equipamentos e produtos – certificação TEMPEST através da capacitação do Centro LUSOCENT e implementação do quadro LUSOCOM e implementação do respetivo plano de certificação	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.1-Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas	1364	PRR	Prazo para manifestação de necessidades de ferramentas de acreditação auditoria de sistemas de informação classificada	30 de julho	SDTI		
		SDTL_P110	Edificação do centro de operações da Competent Public Regulated Service Authority (CPA)	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.4-Capacidade Criptográfica Nacional	19,8	PRR	Implementar plano de certificação TEMPEST	29 de setembro	SDTI		
		SDTL_P111	Certificar e implementar um modelo de preservação digital de informação com requisitos especiais de segurança, referentes aos Processos de Credenciação	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação, submedida TD C19.03.2.5-Certificar e implementar um modelo de preservação digital de informação com requisitos especiais de segurança	1368	PRR	Deployment pela EUSPA da rede GRON (Galileo Robust Operational Network) no centro de operações da CPA	31 de junho			
						PRR	Formação de 2 operadores da CPA	31 de julho	SDTI		
							Emissão do Statement of Compliance das salas e infraestruturas do GNS, para receber o POCP	30 de abril			
							Desenvolvimento aplicacional do Interface gráfico e de gestão base de dados	31 de agosto			
							Certificação do Software aplicacional	29 de dezembro	SDTI		
					Entrega de 20.000 processos de credenciação por parte do GNS à INCM	29 de setembro					
					Digitalização de 20.000 processos de credenciação	29 de dezembro					

Públicos

PA 2023 GNS/CNCS - OBJETIVOS ESTRATÉGICOS E OPERACIONAIS

OBJETIVOS ESTRATÉGICOS				Objetivos operacionais						OBS.
Enunciado	Linhas de ação	Código	Projeto	Objetivo PRR	Meta PRR	Fonte de Financiamento	Tipologia	Meta 2023	EPR Operacional	EPR Normativa
P1	Modernizar a forma como prestamos o serviço e somos percebidos pelos nossos públicos de interesse	SDTL_P113	Prosseguir com a criação da framework para materialização da capacidade para o desempenho das funções de entidade supervisora e de entidade gestora das listas de confiança, definidas pelo Regulamento (UE) n.º 910/2014 (eIDAS)	N/A	N/A	OE	Apresentação de proposta de normativo que define as regras de notificação de incidentes de segurança no que concerne ao consignado no artigo 19.º do Regulamento eIDAS	31 de março	SD11	
			Desenvolvimento de Norma Técnica (NT) e atualização da Norma Técnica (NT) de Segurança Física de Infraestruturas que garantem proteção à Informação Classificada (IC)	N/A	NA	OE	Apresentação de proposta de revisão do normativo relativo à identificação de pessoas físicas através de procedimentos de identificação à distância com recurso a videoconferência	29 de setembro		
			Implementação do Multi Factor Authentication (MFA)	N/A	N/A	OE	Prazo para apresentação da proposta de Norma Técnica (NT)	30 de junho		
			Implementação do Dual Boot	N/A	N/A	OE	Prazo para apresentação da proposta de atualização das Listas de Verificação (LV) no âmbito da Segurança Física de Infraestruturas	31 de março		
							Implementação do Final Operational Capability (FOC)	31 de março		
P2	Incrementar a rede de parceiros (Setor público, Universidade e Politécnicos, Rede de CEOs, Rede de Prestadores de Serviços de confiança, Associações empresariais). Inovar na forma de dar formação, investindo numa lógica de proximidade.	IRC_P116							IRC	
		IRC_P117	Atualização do hardware da atual Rede Interna para futura integração na Rede Classificada ECI/DE	Medida TD C19.03.1-Aumentar a capacidade em cibersegurança e segurança da informação submedida TD C19.03.2.1-Incrementar a certificação e a acreditação de segurança de sistemas e infraestruturas	1364	PRR	Data término de validação da arquitetura para a Rede ECI/DE	31 de março	IRC	
							Porcentagem de Edificação da Rede ECI/DE, grupo criptografia dos segmentos High, Low Level e capilidade eSEIF	25%		
		DCTO_P118	Operacionalização da plataforma de comunicações	N/A	N/A	OE	Registos de comunicação intra ISAC (centros de análise e partilha de informação) na plataforma de comunicações	31 de outubro	CNCS/DCTO	
			Implementação do plano comunicacional no procedimento operacional	N/A	N/A	OE	Plano implementado	31 de outubro		
		DRSC_P120	Formação de auditores especializados	Medida TD C19.03.3-Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação da informação submedida TD C19.03.3.1- Supervisão	1371	PRR	Número de Certificados de formação	8	CNCS/DRSC	
			Normativo setorial - OSE Energia - entrega de proposta final	N/A	N/A	OE	Entrega de proposta final de normativo setorial para validação pela Tuda	31 de junho		
		DRSC_P121	Acreditação de organismos de certificação da conformidade com o QNRCS na AP	Medida TD C19.03.3-Implementar o quadro nacional de Cibersegurança e transformar o atual modelo de coordenação da informação submedida TD C19.03.3.2- Certificação em Cibersegurança	1372	PRR	Número de organismos acreditados	2	CNCS/DRSC	
			Implementação de sistema de gestão de acessos privilegiados	N/A	N/A	OE	Entrada em produção	30 de dezembro		
P3	Capacitar para fazer face aos novos desafios	DST_P123	Centralização de logs de toda a rede	N/A	N/A	OE	Entrada em produção	30 de junho	CNCS/DST	
		DC_P301	Garantir a desmaterialização dos processos de credenciação submedidos (pessoas singulares e coletivas)	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Ciclo de Vida da Informação submedida TD C19.03.2.2- Credenciação de segurança (CREDO)	1389	PRR	Porcentagem dos processos desmaterializados	80%	DC	
			Estabelecer protocolos com Entidades nacionais que podem colaborar nos processos de credenciação a pessoas coletivas e pessoas singulares	N/A	N/A	OE	Número de novas entidades a participar no processo de investigação de segurança	2		

OBJETIVOS ESTRATÉGICOS			Objetivos operacionais							OBS.		
Enunciado	Linhas de ação	Código	Projeto	Indicador				EPR Operativa	EPR Nominal	OBS.		
				Objetivo PRR	Meta PRR	Fonte de Financiamento	Tipologia				Meta 2023	
2	Capacitar para a gestão da informação como potenciador da estratégia	NAD_P303	Implementar o Quadro Nacional de Cibersegurança e transformar o atual modelo de coordenação da cibersegurança e da segurança da informação, alcançando a Initial Operability Capability (IOC) do modelo	Medida TD C19.03.3-Implementar o quadro nacional de cibersegurança, submedida TD C19.03.3.5- Modelo Integrado e Hieroperável de Governação para a Segurança dos Dados, da Informação e do Conhecimento	PRR	1377	N/A	OE	A elaboração do Plano para a IOC	Alcançar o IOC até 31 março	NAD	
		IA_G201	Desenvolver um Sistema de Gestão e Controlo da Atividade Inspetiva e de Auditoria (GAIA)	N/A	OE	N/A	N/A	OE	Percentagem de desenvolvimento do Projeto (De acordo com Plano de Desenvolvimento e Implementação)	100%	IA	
		NAD_G202	Desenvolvimento de novas funcionalidades e melhorias do sistema CRESO (CRESO+)	Medida TD C19.03.2-Incrementar a Segurança na Gestão do Risco Operacional da Infraestrutura de Segurança (CRESO)	PRR	1369	N/A	PRR	Taxa de execução da implementação das novas funcionalidades	70%	NAD	
		NAD_G203	Promover a cultura organizacional através da motivação dos trabalhadores (Nº de atividades)	N/A	OE	N/A	N/A	OE	Número de atividades de team building	2	NAD	
		DST_G204	Construção de Plano de continuidade de negócio	N/A	OE	N/A	N/A	OE	Aprovação da documentação de suporte e restantes evidências técnicas	31 de dezembro	CNCS/DST	
Génética	Robustecer a capacidade e a resiliência organizacional	NAD_G301	Elaboração do Programa Preliminar para a Requalificação e habilitação das novas instalações do GNS/CNCS	Medida TD C19.03.4-Criar as condições físicas e tecnológicas, submedida TD C19.03.4.1- Recuperação e requalificação de infraestruturas e instalação dos serviços	PRR	1380	N/A	PRR	Data de entrega do Programa Preliminar	31 de maio	NAD	
		NAD_G302	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	Medida TD C19.03.4-Criar as condições físicas e tecnológicas, submedida TD C19.03.4.1- Recuperação e requalificação de infraestruturas e instalação dos serviços	PRR	1380	N/A	PRR	Data de lançamento do Procedimento Concursal	31 de julho	NAD	
		NAD_G303	Reforçar a Segurança Física das instalações	N/A	OE	N/A	N/A	OE	Resolução de anomalias no Sistema de Detecção de Intrusão (SDI)	30 de junho	OfSeg	
		NAD_G304	Reforço do treino de Segurança	N/A	OE	N/A	N/A	OE	Reforço da capacidade de leitura e fiabilidade do Sistema de Controlo de Acessos (SCA) nos pontos	31 de outubro	OfSeg	

ANEXO F

PÁGINA DEIXADA EM BRANCO

PÁGINA DEIXADA EM BRANCO

ANEXO G

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

PLANO DE FORMAÇÃO PARA 2023

PÁGINA DEIXADA EM BRANCO

Plano de Formação para 2023

GNS

ID	Un. Org.	Formação	Participantes	Local	Zona	Data de início	Total de horas de formação	Total de dias da missão	Nº de Pessoas	Chefe da Equipa	ESTIMATIVA DE CUSTOS					Prioridade na Unidade Orgânica	Custo total Propinas + Inscrição		
											02.02.13	01.02.04		TOTAL					
											02.02.15/A/B	Formação (propinas e inscrição PP)	Transporte		Alojamento	Portagens e Tx. Cidade	Ajudas de custo		
GNS/2023/F/P1/01	AND	Crypto Administration		NCIA - Oeiras	PT-LX	TBD	40	5	3	MIL - OFSUB / SMOR / SCH		1 160,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	3 480,00 €
GNS/2023/F/P1/02	AND	CARDS for NATO Crypto Custodian		NCIA - Oeiras	PT-LX	TBD	40	5	3	MIL - OFSUB / SMOR / SCH		1 160,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2	3 480,00 €
GNS/2023/F/P1/03 *	AND	EU COMSEC Training Seminar		GSC, Bruxelas	EU	TBD	16	2	3	MIL - OFGEN / OFSUP		0,00 €	1 800,00 €	1 200,00 €	15,00 €	500,35 €	3 515,35 €	3	0,00 €
GNS/2023/F/P1/04	AND	NATO CIS Security Officer		NCIA-Oeiras	PT-LX	TBD	40	5	1	MIL - OFGEN / OFSUP		880,00 €	0,00 €	0,00 €	0,00 €	0,00 €	880,00 €	4	880,00 €
GNS/2023/F/P1/05*	AND	NATO KMI Management Client Operator's Training		Maryland, USA	Fora EU	01/08/2023	80	10	1	MIL - OFSUB / SMOR / SCH		0,00 €	1 300,00 €	4 500,00 €	45,00 €	782,67 €	6 627,67 €	5	0,00 €
GNS/2023/F/P1/06	IA	Técnico de Security		APSEI	PT-LX	TBD	50	5	3	MIL - OFGEN / OFSUP		1 162,00 €	0,00 €	0,00 €	0,00 €	0,00 €	3 486,00 €	1	3 486,00 €
GNS/2023/F/P1/07	IA	Sistemas de Proteção Perimétrica		APSEI	PT-LX	TBD	12	5	3	MIL - OFGEN / OFSUP		239,00 €	0,00 €	0,00 €	0,00 €	0,00 €	717,00 €	2	717,00 €
GNS/2023/F/P1/08	OFSEG	Redes Informáticas Aplicadas aos Sistemas Electronicos de Segurança		APSEI, On-line	PT-LX	TBC	7	2	1	MIL - OFGEN / OFSUP		143,00 €	0,00 €	0,00 €	0,00 €	0,00 €	143,00 €	5	143,00 €
GNS/2023/F/P1/09	OFSEG	Sensibilização em Primeiros Socorros (7 horas)		GNS	PT-LX	TBD	7	1	12	MIL - OFGEN / OFSUP		660,00	0,00 €	0,00 €	0,00 €	0,00 €	7 920,00 €	1	7 920,00 €
GNS/2023/F/P1/10	OFSEG	Sensibilização em Primeiros Socorros (7 horas)		GNS	PT-LX	TBD	7	1	12	MIL - OFGEN / OFSUP		660,00	0,00 €	0,00 €	0,00 €	0,00 €	7 920,00 €	2	7 920,00 €
GNS/2023/F/P1/11	OFSEG	Sensibilização em Combate a Incêndios e Evacuação de Edifícios (7 horas)		ENB - Sintra	PT-LX	TBD	16	1	16	MIL - OFGEN / OFSUP		1160,00	0,00 €	0,00 €	0,00 €	0,00 €	18 560,00 €	3	18 560,00 €
GNS/2023/F/P1/12	OFSEG	Evacuação de Edifícios		APSEI, On-line	PT-LX	TBC	7	1	1	MIL - OFSUB / SMOR / SCH		156,00 €	0,00 €	0,00 €	0,00 €	0,00 €	156,00 €	4	156,00 €
GNS/2023/F/P1/13 *	DSDTI - ST	Network Security Course		Obermammegau	Fora EU	30/01/2023	70/32	12	1	MIL - OFSUB / SMOR / SCH		3 500,00 €	1 300,00 €	5 500,00 €	55,00 €	939,20 €	11 294,20 €	1	3 500,00 €
GNS/2023/F/P1/14 *	DSDTI - ST	Tempest & EMC Training		Aachen	EU	28/08/2023	35	7	2	MIL - OFGEN / OFSUP		5 000,00 €	1 200,00 €	4 800,00 €	60,00 €	1 167,47 €	17 227,47 €	2	10 000,00 €
GNS/2023/F/P1/15 *	DSDTI - ST	CC Certification		Bonn	EU	08/05/2023	35	7	2	MIL - OFGEN / OFSUP		3 800,00 €	1 200,00 €	4 800,00 €	60,00 €	1 167,47 €	14 827,47 €	4	7 600,00 €
GNS/2023/F/P1/16	DSDTI - ST	Curso Licenciatura		LX	PT-LX	01/10/2023	ano letivo	0	1	MIL - OFGEN / OFSUP		800,00 €	0,00 €	0,00 €	0,00 €	0,00 €	800,00 €	14	800,00 €
GNS/2023/F/P1/17	DSDTI - SC	Risk Management 31000 Lead Manager		On-line/Lx	PT-LX	TBD	40	5	1	MIL - OFGEN / OFSUP		2 610,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 610,00 €	10	2 610,00 €
GNS/2023/F/P1/18	DSDTI - SC	Risk Management 27005 Manager		On-line/Lx	PT-LX	TBD	16	2	1	MIL - OFGEN / OFSUP		1 315,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 315,00 €	11	1 315,00 €
GNS/2023/F/P1/19	DSDTI - SC	Risk Management 27005 Risk Methodologies		On-line/Lx	PT-LX	TBD	40	5	1	MIL - OFGEN / OFSUP		2 910,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 910,00 €	12	2 910,00 €
GNS/2023/F/P1/20	DSDTI - SC	Information Security 27035 Incident Manager		On-line/Lx	PT-LX	TBD			1	MIL - OFGEN / OFSUP		1 250,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 250,00 €	13	1 250,00 €
GNS/2023/F/P1/21	DSDTI - SI	Gestor de Security		On-line/Lx	PT-LX	TBD	50	0	2	MIL - OFGEN / OFSUP		1 313,00 €	0,00 €	0,00 €	0,00 €	0,00 €	2 626,00 €	15	2 626,00 €
GNS/2023/F/P1/22 *	DSTI - SI	Sistemas de videovigilância - Avançado		On-line/Lx	PT-LX	TBD	24	0	2	MIL - OFGEN / OFSUP		689,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 378,00 €	16	1 378,00 €
GNS/2023/F/P1/23 *	DSTI - SE	Gallieu Security Monitor Center - GRON Operators		Paris	EU	05/04/2023	32	5	3	MIL - OFGEN / OFSUP		0,00 €	1 800,00 €	4 800,00 €	60,00 €	1 250,87 €	7 910,87 €	3	0,00 €

Plano de Formação para 2023

GNS

ID	Un. Org.	Formação	Participantes	Local	Zona	Data de início	Total de horas de formação	Total de dias da missão	Nº de Pessoas	Chefe da Equipa	ESTIMATIVA DE CUSTOS						Prioridade na Unidade Orgânica	Custo total Propinas + Inscrição
											FF	02.02.15.A/B Formação (propinas e Inscrição PP)	Transporte	Alojamento	Portagens e Tx. Cidade	01.02.04 Ajudas de custo		
GNS/2023/F/P1/24	DSDTI - SC	Information Security 27034 - Lead Auditor		On-line/Lx	PT-LX	TBC	40	5	1	MIL - OFGEN / OFSUP	GNS/RP	2 480,00 €	0,00 €	0,00 €	0,00 €	2 480,00 €	5	2 480,00 €
GNS/2023/F/P1/25	DSDTI - SC	Information Security 27002 Lead Control Manager		On-line/Lx	PT-LX	TBC	40	5	1	MIL - OFGEN / OFSUP	GNS/RP	2 480,00 €	0,00 €	0,00 €	0,00 €	2 480,00 €	6	2 480,00 €
GNS/2023/F/P1/26	DSDTI - ST	Cloud Security Professional		On-line/Lx	PT-LX	TBC	35	5	1	MIL - OFGEN / OFSUP	GNS/RP	2 555,00 €	0,00 €	0,00 €	0,00 €	2 555,00 €	9	2 555,00 €
GNS/2023/F/P1/27	DSDTI - SC	EU Data Protection Officer DPO		Behavior	PT-LX	TBC	24	3	1	MIL - OFGEN / OFSUP	GNS/RP	1 860,00 €	0,00 €	0,00 €	0,00 €	1 860,00 €	7	1 860,00 €
GNS/2023/F/P1/28	DSDTI - SC	Data Protection 27701 Lead Auditor		On-line/Lx	PT-LX	TBC	40	5	1	MIL - OFGEN / OFSUP	GNS/RP	2 610,00 €	0,00 €	0,00 €	0,00 €	2 610,00 €	17	2 610,00 €
GNS/2023/F/P1/29	DSDTI - SC	Certified Chief Information Security Officer (CCISO)		On-line/Lx	PT-LX	TBC	40	5	1	MIL - OFGEN / OFSUP	GNS/RP	3 270,00 €	0,00 €	0,00 €	0,00 €	3 270,00 €	18	3 270,00 €
GNS/2023/F/P1/30	DSDTI - SC	Information Security Manager (CISM Preparation Course)		On-line/Lx	PT-LX	TBC	24	3	1	MIL - OFGEN / OFSUP	GNS/RP	1 950,00 €	0,00 €	0,00 €	0,00 €	1 950,00 €	19	1 950,00 €
GNS/2023/F/P1/31 *	DSDTI - SC	Cybersecurity Profissional		On-line/Lx	PT-LX	10/03/2023	16	2	1	MIL - OFGEN / OFSUP	GNS/RP	1 650,00 €	0,00 €	0,00 €	0,00 €	1 650,00 €	20	1 650,00 €
GNS/2023/F/P1/32 *	DSTI - SI	Redes Informáticas Aplicadas aos Sistemas Electronicos de Segurança		On-line/Lx	PT-LX	TBD	7	1	1	MIL - OFGEN / OFSUP	GNS/RP	260,00 €	0,00 €	0,00 €	0,00 €	260,00 €	21	260,00 €
GNS/2023/F/P1/33 *	DSDTI - ST	Nato Security Course		Oberammergau	EU	04/12/2023	35	6	2	MIL - OFGEN / OFSUP	PRR	1 650,00 €	1 200,00 €	4 000,00 €	50,00 €	9 550,69 €	8	3 300,00 €
GNS/2023/F/P1/34 *	DC	Nato Security Course		Oberammergau	EU	04/12/2023	35	6	1	MIL - OFGEN / OFSUP	PRR	1 650,00 €	600,00 €	2 000,00 €	25,00 €	4 775,35 €	1	1 650,00 €
GNS/2023/F/P1/35	DC	Adobe Acrobat Professional		Lisboa	PT-LX	TBD	12	0	1	CIV - INF NIVEL 9	GNS/RP	1 390,00 €	0,00 €	0,00 €	0,00 €	1 390,00 €	2	1 390,00 €
GNS/2023/F/P1/36	IRC	Check Point Administrator and Troubleshooting (CCSA+ CCTA)		Rumos, LX	PT-LX	08/05/2023	35	5	1	MIL - SA / 1SAR / 2SAR	GNS/RP	3 259,50 €	0,00 €	0,00 €	0,00 €	3 259,50 €	1	3 259,50 €
GNS/2023/F/P1/37	IRC	Red Hat System Administration II (RH134)		Rumos, LX	PT-LX	13/03/2023	34	5	2	MIL - OFSUB / SMOR / SCH	GNS/RP	5 694,90 €	0,00 €	0,00 €	0,00 €	11 389,80 €	2	11 389,80 €
GNS/2023/F/P1/38	IRC	Check Point Troubleshooting Administrator (CCTA)		Rumos, LX	PT-LX	11/05/2023	14	2	1	MIL - OFSUB / SMOR / SCH	GNS/RP	1 820,40 €	0,00 €	0,00 €	0,00 €	1 820,40 €	3	1 820,40 €
GNS/2023/F/P1/39	IRC	Administração e Configuração de Windows Server 2019		Rumos, LX	PT-LX	19/06/2023	35	5	2	MIL - OFSUB / SMOR / SCH	GNS/RP	3 493,20 €	0,00 €	0,00 €	0,00 €	6 986,40 €	4	6 986,40 €
GNS/2023/F/P1/40	IRC	Máquinas de cifra - TCE		EMGFA - Lisboa	PT-LX	01/07/2020	1	2	4	MIL - OFSUB / SMOR / SCH	GNS/RP	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	5	0,00 €
GNS/2023/F/P1/41	IRC	VMware vSphere: What's New [V6.7 to V7]		Rumos, LX	PT-LX	04/12/2023	24	3	1	MIL - SA / 1SAR / 2SAR	GNS/RP	2 177,10 €	0,00 €	0,00 €	0,00 €	2 177,10 €	6	2 177,10 €
GNS/2023/F/P1/42	IRC	AZ-040: Automating Administration with PowerShell		Rumos, LX	PT-LX	11/09/2023	35	5	1	MIL - OFSUB / SMOR / SCH	GNS/RP	2 177,10 €	0,00 €	0,00 €	0,00 €	2 177,10 €	7	2 177,10 €
GNS/2023/F/P1/43	IRC	Mestrado Engenharia Informática - eLearning - Pós Laboral		Univ. Evora, Evora	PT-LX	01/10/2023			1	MIL - OFSUB / SMOR / SCH	GNS/RP	1 050,00 €	0,00 €	0,00 €	0,00 €	1 050,00 €	8	1 050,00 €
GNS/2023/F/P1/44	IRC	ITIL 4 Foundation		Rumos, LX	PT-LX	(a confirmar)	21	3	1	MIL - OFSUB / SMOR / SCH	GNS/RP	1 704,78 €	0,00 €	0,00 €	0,00 €	1 704,78 €	9	1 704,78 €
GNS/2023/F/P1/45	IRC	Mestrado Engenharia Informática - Pós Laboral 1ano		IP Leiria	PT-LX	01/01/2023			1	MIL - SA / 1SAR / 2SAR	GNS/RP	630,00 €	0,00 €	0,00 €	0,00 €	630,00 €	10	630,00 €
GNS/2023/F/P1/46	IRC	Mestrado Engenharia Informática - Pós Laboral		IP Leiria	PT-LX	15/09/2023			1	MIL - SA / 1SAR / 2SAR	GNS/RP	1 140,00 €	0,00 €	0,00 €	0,00 €	1 140,00 €	11	1 140,00 €
GNS/2023/F/P1/47	IRC	Certified SOC Analyst (CSA)		Rumos, LX	PT-LX	(a confirmar)	24	3	1	MIL - SA / 1SAR / 2SAR	GNS/RP	2 583,00 €	0,00 €	0,00 €	0,00 €	2 583,00 €	12	2 583,00 €

Plano de Formação para 2023

GNS

ID	Un. Orgâ.	Formação	Participantes	Local	Zona	Data de início	Total de horas de formação	Total de dias da missão	Nº de Pessoas	Chefe da Equipa	ESTIMATIVA DE CUSTOS						Prioridade na Unidade Orgânica	Custo total - Propinas + Inscrição	
											02.02.15/A/B	02.02.13		01.02.04		TOTAL			
											FF	Formação (propinas e Inscrição PP)	Transporte	Alojamento	Portagens e Tx. Cidade		Ajudas de custo		
GNS/2023/F/P1/48	IRC	CompTIA Cybersecurity Analyst		Rumos, LX	PT-LX	09/10/2023	35	5	1	MIL - SAI / 1SAR / 2SAR	GNS/RP	2 644,50 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	13	2 644,50 €
GNS/2023/F/P1/49	NAD	Preparação e redação de atos legislativos e regulamentos		INA	PT-LX	30jan - 03fev	21	3	1	MIL - OFGEN / OFSUP	GNS/RP	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	210,00 €
GNS/2023/F/P1/50	NAD	Curso de Proteção de Dados Pessoais em e-learning		NOVA School of Law (Faculdade de Direito da Universidade Nova de Lisboa)	PT-LX	21-29nov	15	4	2	MIL - OFGEN / OFSUP	GNS/RP	250,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	500,00 €
GNS/2023/F/P1/51	NAD	Mestrado em Segurança de Informação e Direito no Ciberespaço		EN/IST/UL	PT-LX	01/10/2023	0	0	1	CIV - SUP NIVEL 18	GNS/RP	5 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €		
GNS/2023/F/P1/52	NAD	Curso de Especialização em Direito do Emprego Público		CEDIPRE/FD/Univ.Coimbra	PT-LX	18/03/2023	0	0	1	CIV - SUP NIVEL 18	GNS/RP	800,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1	800,00 €

Plano de Formação para 2023

CNCS

ID	Un. Orgâ.	Formação	Participantes	Local	Zona	Data de início	Total de horas de formação	Total de dias da missão	Nº de Pessoas	Chefe da Equipa	ESTIMATIVA DE CUSTOS						Prioridade na Unidade Orgânica	Custo total Propinas + Inscrição	
											FF	02.02.15.A/B Formação (propinas e inscrição PP)	Transporte	Alojamento	Portagens e Tx. Cidade	01.02.04 Ajudas de custo			TOTAL
	DST	Curso SANS a designar			EU	05/08/2023	48	7	5	CIV - SUP NIVEL 18	PRR	6 950,00 €	3 000,00 €	12 000,00 €	150,00 €	2 189,08 €	52 089,08 €	1	34 750,00 €
	DST	Formação a designar - Área de Sistemas			PT-CONT	20/03/2023	40	5	3	CIV - SUP NIVEL 18	PRR	2 500,00 €	240,00 €	900,00 €	0,00 €	750,30 €	9 390,30 €	1	7 500,00 €
	DST	Formação a designar - Área de Redes/Segurança			PT-CONT	19/06/2023	40	5	1	CIV - SUP NIVEL 18	PRR	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	2 500,00 €
	DST	Formação a designar - SOC			PT-CONT	19/06/2023	40	5	1	CIV - SUP NIVEL 18	PRR	2 500,00 €	80,00 €	300,00 €	0,00 €	250,10 €	3 130,10 €	1	2 500,00 €
	DCTO	SANS MGT514: Security Strategic Planning, Policy, and Leadership (P1)			EU	01/04/2023	35	6	3	CIV - SUP NIVEL 18	PRR	7 170,00 €	1 800,00 €	6 000,00 €	75,00 €	1 125,81 €	30 510,81 €	1	21 510,00 €
	DCTO	SANS SEC530: Defensible Security Architecture and Engineering: Implementing Zero Trust for the Hybrid Enterprise (P1)			EU	01/10/2023	35	6	1	CIV - SUP NIVEL 18	PRR	7 170,00 €	600,00 €	2 000,00 €	25,00 €	375,27 €	10 170,27 €	1	7 170,00 €
	DCTO	SANS SEC566: Implementing and Auditing Security Frameworks and Controls (P1)			EU	01/10/2023	35	6	2	CIV - SUP NIVEL 18	PRR	7 170,00 €	1 200,00 €	4 000,00 €	50,00 €	750,54 €	20 340,54 €	1	14 340,00 €
	DDI	Curso de Especialização – “ISO 27001 Implementer Foundation”			Online	01/04/2023	16	3	1	CIV - SUP NIVEL 18	PRR	830,00 €	0,00 €	0,00 €	0,00 €	0,00 €	830,00 €	1	830,00 €
	DDI	SEC487: Open-Source Intelligence (OSINT) Gathering and Analysis			Online	01/04/2023	50	6	1	CIV - SUP NIVEL 18	PRR	8 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8 000,00 €	1	8 000,00 €
	DDI	Executive Master em Gestão de Programas e Projetos			PT-LX	01/09/2023	200		1	CIV - SUP NIVEL 18	PRR	8 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8 000,00 €	1	8 000,00 €
	DDI	MGT521: Leading Cybersecurity Change-Building a Security-Based Culture ministrada pelo SANS			PT-LX	01/07/2023	45	5	1	CIV - SUP NIVEL 18	PRR	8 000,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8 000,00 €	1	8 000,00 €
	DDI	Gestão Aplicada de Projetos			PT-LX	01/05/2023	16	2	1	CIV - SUP NIVEL 18	OE	1 250,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 250,00 €	1	1 250,00 €
	DDI	Formação Avançada em Gestão de Reputação e Comunicação de Crise			PT-LX	01/03/2023	49		1	CIV - SUP NIVEL 18	OE	1 250,00 €	0,00 €	0,00 €	0,00 €	0,00 €	1 250,00 €	1	1 250,00 €
	DRSC	Código do Procedimento Administrativo		Online	Online	02/05/2023	21	3	4	CIV - SUP NIVEL 18	PRR	210,00 €	0,00 €	0,00 €	0,00 €	0,00 €	840,00 €	1	840,00 €
	DRSC	Curso Prático Intensivo de Direito das Contraordenações		Online	Online	27/03/2023	20	3	4	CIV - SUP NIVEL 18	PRR	198,00 €	0,00 €	0,00 €	0,00 €	0,00 €	792,00 €	1	792,00 €
	DRSC	Família ISO 27000 (incluída no Programa de formação Auditores ANCC + RISC - ver lista de compras)		Online	Online	01/10/2023	35	5	10	CIV - SUP NIVEL 18	PRR	2 398,00 €	0,00 €	0,00 €	0,00 €	0,00 €	23 980,00 €	1	23 980,00 €
	DRSC	ISO/IEC 15408 + 18045 + EUCC (incluída no Programa de formação Auditores ANCC + RISC - ver lista de compras)		Online	Online	01/10/2023	35	5	6	CIV - SUP NIVEL 18	PRR	2 398,00 €	0,00 €	0,00 €	0,00 €	0,00 €	14 388,00 €	1	14 388,00 €
												7 000,00 €	25 500,00 €	300,00 €	5 691,20 €	196 091,20 €	1	0,00 €	

ANEXO H

GABINETE NACIONAL DE SEGURANÇA E CENTRO NACIONAL DE CIBERSEGURANÇA

QUAR 2023

PÁGINA DEIXADA EM BRANCO

Quadro de Avaliação e Responsabilização

ANO:2023

Presidência do Conselho de Ministros

Gabinete Nacional de Segurança-PCM

MISSÃO: -Garantir a segurança da informação classificada no âmbito nacional e das organizações internacionais de que Portugal é parte e exercer a função de autoridade de credenciação de pessoas e empresas 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 Electronica do Estado - Infra - Estrutura de Chaves Públicas (SCEE).

- 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.

Objectivos Estratégicos

DESIGNAÇÃO	META 2023	TAXA REALIZAÇÃO
Capacitar os públicos de interesse para os desafios da sociedade do conhecimento		
Robustecer a capacidade de conhecimento do ciberespaço relevante e de proteção da sociedade.		
Modernizar a forma como prestamos o serviço e somos percecionados pelos nossos públicos de interesse		
Investir na formação e no bem-estar dos colaboradores		

Objectivos Operacionais

Eficácia

Peso: 20.0

Contratualização dos Centros de Competência (Nº de contratualizações)									Peso: 50.0
INDICADORES	2021	2022	META 2023	Tolerância	Valor Crítico	PESO	RESULTADO	TAXA REALIZAÇÃO	CLASSIFICAÇÃO
Número de contratos formalizados			3.00	1.00	5.00	100			
Caracterização de Entidades OSE e AP									Peso: 50.0
INDICADORES	2021	2022	META 2023	Tolerância	Valor Crítico	PESO	RESULTADO	TAXA REALIZAÇÃO	CLASSIFICAÇÃO
Número de entidades caracterizadas			40.00	5.00	56.00	100			

Eficiência

Peso: 40.0

Otimizar a utilização das instalações do "SubRegisto as a Service"									Peso: 50.0
INDICADORES	2021	2022	META 2023	Tolerância	Valor Crítico	PESO	RESULTADO	TAXA REALIZAÇÃO	CLASSIFICAÇÃO
Conclusão das melhorias nas infraestruturas do "SubRegisto as a service" (dias)			200.00	15.00	139.00	50			
Initial Operability Capability (IOC). (dias)			300.00	15.00	214.00	50			
Promover a melhoria dos processos através do desenvolvimento da máquina de cifra HSM-T2 para nova versão 2.1.									Peso: 50.0
INDICADORES	2021	2022	META 2023	Tolerância	Valor Crítico	PESO	RESULTADO	TAXA REALIZAÇÃO	CLASSIFICAÇÃO
Desenho de novo algoritmo de chaves internas mais robusto, ligação externa para programação e carregamento de chaves, botão ZEROID, e revestimento de proteção para operações em ambientes desfavoráveis.			260.00	15.00	184.00	50			
Plano de industrialização para o fabrico de 100 unidades			260.00	15.00	185.00	50			

Quadro de Avaliação e Responsabilização

Objectivos Operacionais

Qualidade

Peso: 40.0

Promover ganhos de eficiência no domínio da formação interna e externa (% índice de satisfação)									Peso: 50.0
INDICADORES	2021	2022	META 2023	Tolerância	Valor Crítico	PESO	RESULTADO	TAXA REALIZAÇÃO	CLASSIFICAÇÃO
Índice de satisfação médio (em %) dos formandos que frequentaram ações de formação ministrada pelo GNS		80.00	85.00	5.00	100.00	100			
Promover a cultura organizacional através da motivação dos trabalhadores (Nº de atividades)									Peso: 50.0
INDICADORES	2021	2022	META 2023	Tolerância	Valor Crítico	PESO	RESULTADO	TAXA REALIZAÇÃO	CLASSIFICAÇÃO
Número de atividades de team building			2.00	1.00	3.00	100			

Recursos Humanos

DESIGNAÇÃO	PONTUAÇÃO	PLANEADOS	REALIZADOS	DESVIO
Dirigentes - Direcção superior *	20.0	60.0		.0
Dirigentes - Direcção intermédia e Chefes de equipa *	16.0	192.0		.0
Outros Oficiais	12.0	156.0		.0
Sargentos	8.0	192.0		.0
Praça	5.0	50.0		.0
Guardas	5.0	20.0		.0
Agente	5.0	15.0		.0
Técnico Superior	12.0	12.0		.0
Assistente Técnico	8.0	32.0		.0
Assistente Operacional *	5.0	10.0		.0
Consultores	12.0	156.0		.0
Técnico	8.0	184.0		.0
		1079.0		

Número de trabalhadores a exercer funções no serviço:

31/12/2022	31/12/2023
113	122

Recursos Financeiros

DESIGNAÇÃO	PLANEADOS (EUROS)	EXECUTADOS	DESVIO
Orçamento de Funcionamento	3222223		
Despesas c/Pessoal	2447654		
Aquisições de Bens e Serviços	404426		
Outras Despesas Correntes			

Quadro de Avaliação e Responsabilização

Recursos Financeiros			
DESIGNAÇÃO	PLANEADOS (EUROS)	EXECUTADOS	DESVIO
Despesas Restantes	370143		
PIDDAC			
Outros Valores	11142996		
TOTAL (OF + PIDDAC + Outros)	14365219		

NOTA EXPLICATIVA

JUSTIFICAÇÃO DE DESVIOS

Avaliação Final

Eficácia	0.0	
Contratualização dos Centros de Competência (Nº de contratualizações)		
Caracterização de Entidades OSE e AP		
Eficiência	0.0	
Otimizar a utilização das instalações do "SubRegisto as a Service"		
Promover a melhoria dos processos através do desenvolvimento da máquina de cifra HSM-T2 para nova versão 2.1.		
Qualidade	0.0	
Promover ganhos de eficiência no domínio da formação interna e externa (% índice de satisfação)		
Promover a cultura organizacional através da motivação dos trabalhadores (Nº de atividades)		

TAXA DE REALIZAÇÃO FINAL	NOTA FINAL
0.0	

Indicadores	Justificação do Valor Crítico
Número de contratos formalizados	
Número de entidades caracterizadas	
Conclusão das melhorias nas infraestruturas do "SubRegisto as a service" (dias)	
Inicial Operability Capability (IOC). (dias)	
Desenho de novo algoritmo de chaves internas mais robusto, ligação externa para programação e carregamento de chaves, botão ZEROID, e revestimento de proteção para operações em ambientes desfavoráveis.	
Plano de industrialização para o fabrico de 100 unidades	
Índice de satisfação médio (em %) dos formandos que frequentaram ações de formação ministrada pelo GNS	O melhor resultado que se pode obter com este indicador é 100%. Considerando que a meta no ano transato foi 80%, considerou-se a meta para 223 de 85%, assim será impossível garantir a formula, assim o valor crítico que tem de evidenciar o limite será de 100%.
Número de atividades de team building	

Indicadores	Fonte de Verificação
Número de contratos formalizados	Contratos celebrados com as entidades

Quadro de Avaliação e Responsabilização

Indicadores	Fonte de Verificação
Número de entidades caracterizadas	IOC das entidades
Conclusão das melhorias nas infraestruturas do "SubRegisto as a service" (dias)	Auto de receção da obras
Inicial Operability Capability (IOC). (dias)	Publicitação do serviço
Desenho de novo algoritmo de chaves internas mais robusto, ligação externa para programação e carregamento de chaves, botão ZEROID, e revestimento de proteção para operações em ambientes desfavoráveis.	Aprovação do desenho do algoritmo por parte do Serviço
Plano de industrialização para o fabrico de 100 unidades	Aprovação do plano de industrialização por parte do Serviço
Índice de satisfação médio (em %) dos formandos que frequentaram ações de formação ministrada pelo GNS	Questionário de satisfação
Número de atividades de team building	Plano anual de realização de ações de team-building

**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