GNS | Gabinete Nacional de Segurança
PORTUGAL

NORMA TÉCNICA – H 03

ACESSO A MATERIAL CRIPTOGRÁFICO

Lisboa, 18 de setembro de 2024

A Autoridade Nacional de Segurança / Autoridade Nacional de Distribuição

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2024.10.17 15:05:31 +01'00'

(António Gameiro Marques)

(Verso em branco)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

1. REFERÊNCIAS

a. Lei Orgânica do Gabinete Nacional de Segurança (GNS):

Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual, republicado em anexo ao Decreto-Lei n.º 136/2017, de 6 de novembro

b. Resolução do Conselho de Ministros:

Resolução do Conselho de Ministros n.º 50/88, de 12 de junho, que aprova as Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas (SEGNAC 1)

c. Normas Técnicas (NT) do GNS:

1) Norma Técnica A 01 – Ficha Individual para Credenciação de Segurança de Pessoal, em qualquer marca e para efeitos do disposto no artigo 9.º da Lei n.º 49/2009, de 07 de janeiro de 2013

2) Norma Técnica A 02 – Credenciação de Segurança de Pessoal Civil e Militar dos Departamentos do Estado e do JHQ Lisbon, de 04 de fevereiro de 2011

3) Norma Técnica E 01 – Marcas, Graus de Segurança, Limites, Designadores e Competências para Classificar Informação, de 04 de setembro de 2023

4) Norma Técnica E 08 – Sistema de Segurança Eletrónica da Informação (SEIF), de 01 de dezembro de 2020

d. Organização do Tratado do Atlântico Norte / *North Atlantic Treaty Organization* (OTAN/NATO):

1) C-M(2002)49-REV1, *Security Within the North Atlantic Treaty Organization*, de 20 de novembro de 2020

2) AC/35-D/2000-REV8, Directive on Personnel Security, de 25 de novembro de 2020

3) SDIP 293/1 - *Instructions for the Control and Safeguarding of NATO Cryptomaterial*, de março de 2011

e. União Europeia / *European Union* (UE/EU):

1) Decisão 2013/488/UE do Conselho, de 23 de setembro de 2013, relativa às Regras de Segurança aplicáveis à proteção das Informações Classificadas da UE

2) IASG 2-03 – *Information Assurance Security Guidelines on the Management of European Union crypto* material and COMSEC items, do Conselho da União Europeia, de 27 de maio de 2022

f. Comunidade Europeia da Energia Atómica / *European Atomic Energy Community* (CEEA/EURATOM):

Decisão 2015/444/EU, EURATOM da Comissão, de 13 de março de 2015, relativa às Regras de Segurança aplicáveis à proteção das Informações Classificadas da UE

g. Agência Espacial Europeia / *European Space Agency* (AEE/ESA):

ESA/REG/004 – *Security Regulations of the European Space Agency*, de 18 de janeiro de 2012

2. DEFINIÇÕES

a. **Autorização Cripto**: Constitui uma permissão formal conferida pelo responsável máximo da organização ou pela entidade que detenha essa competência delegada dentro da organização, a um individuo, para manusear material criptográfico. A atribuição da Autorização Cripto pressupõe a existência de uma necessidade de conhecer válida, bem como a titularidade de um Certificado de Credenciação de Segurança Pessoal (CCSP) válido, que inclua o designador de categoria especial CRIPTO/*CRYPTO* (não aplicável à marca UE) para o grau de classificação de segurança do material criptográfico a manusear.

b. **Certificado de Credenciação de Segurança do Pessoal (CCSP)**: Habilitação de segurança concedida a um indivíduo em função da sua "necessidade de conhecer", determinada pelo responsável máximo da organização a que pertence ou pela entidade que detenha essa competência delegada dentro da organização, após validação da Autoridade Nacional de Segurança (ANS).

c. **Equipamento criptográfico**: Qualquer dispositivo ou mecanismo que empregue um processo criptográfico para proteger a confidencialidade, integridade, disponibilidade, autenticidade ou não-repúdio da informação.

d. **Material criptográfico**: Compreende material-chave em qualquer dos formatos (chaves físicas ou eletrónicas, códigos e sistemas de autenticação), publicações (instruções de operação, manuais e registos de manutenção), equipamentos e dispositivos associados, elementos essenciais para o processo de encriptação/desencriptação ou autenticação das comunicações e necessários para manter a confidencialidade, integridade, disponibilidade, autenticidade ou não-repúdio da Informação Classificada (IC) dos Sistemas de Informação e Comunicações (SIC) de índole nacional e das organizações internacionais (OI) de que Portugal faça parte.

e. **Segurança Criptográfica**: Consiste no conjunto de medidas de segurança, tais como segurança física, procedimentos e técnicas, aplicado ao material criptográfico, de forma a garantir a proteção da IC contra a exploração por parte de pessoas não autorizadas. O sucesso da segurança criptográfica depende da utilização adequada de sistemas criptográficos, de acordo com as instruções de operação especificas de cada sistema, bem como na observância dos requisitos processuais detalhados em NT do GNS e Instruções para o controlo e salvaguarda do Material Criptográfico emanadas pelas OI de que Portugal faça parte. No âmbito da presente NT será igualmente utilizada a designação Segurança das Comunicações (SEGCOM), cujo significado será equivalente ao atribuído para a Segurança Criptográfica.

f. **Sistema Criptográfico**: Consiste na combinação de itens de material criptográfico, que utilizados em conjunto, funcionam como um mecanismo criptográfico destinado a garantir a confidencialidade, integridade, disponibilidade, autenticidade ou não-repúdio da informação processada pelos SIC de índole nacional e das OI de que Portugal faça parte. Os sistemas criptográficos podem utilizar métodos de cifra *online* ou *offline*.

g. **Sistema Criptográfico de Alto Grau**: Sistemas criptográficos que fornecem uma segurança duradoura à informação neles processada, sendo altamente resistentes a análise criptológica, por um período indefinido ou consideravelmente longo.

h. **Sistema Criptográfico de Baixo Grau**: Sistemas criptográficos concebidos para utilização quando não estejam disponíveis, ou não sejam aplicáveis, outros sistemas mais seguros, fornecendo apenas uma proteção limitada. Estes sistemas são vocacionados para aplicações táticas, onde seja fundamental obter alguma proteção de segurança, mas onde a rapidez e a simplicidade de operação sejam requisitos prioritários. São exemplos os códigos táticos e os equipamentos portáteis.

3. SITUAÇÃO

a. Os requisitos de segurança para proteção de material criptográfico são idênticos aos requisitos de segurança aplicáveis à proteção de IC, contudo, pela natureza sensível do material criptográfico, são necessários controlos adicionais, a fim de prevenir que pessoas não autorizadas tenham acesso, ou retirem vantagem desse acesso que possibilite a criptoanálise e providencie conhecimento de procedimentos e técnicas criptográficas.

b. O acesso a material criptográfico deve restringir-se a indivíduos expressamente autorizados e que tenham uma justificável necessidade de conhecer para o cabal desempenho das suas funções.

c. Os indivíduos que no âmbito das suas funções necessitem de ter acesso regular a material criptográfico no grau de CONFIDENCIAL ou superior, da marca NACIONAL ou de OI de que Portugal faça parte, têm de ser titulares de CCSP válido, que inclua o designador de categoria especial CRIPTO/*CRYPTO*. No caso particular da UE, a titularidade de um CCSP válido em conformidade com o mais elevado grau de classificação de segurança do material criptográfico a manusear será suficiente.

4. OBJETO / FINALIDADE

Esta norma destina-se a definir os requisitos e os procedimentos necessários, a observar pelas entidades de natureza pública ou privada, para que o seu pessoal tenha acesso a material criptográfico, destinado a proteger IC de índole nacional, ou de OI de que Portugal faça parte.

5. ÂMBITO

A presente norma aplica-se a todas as entidades de natureza pública ou privada, quer em Território Nacional, quer no exterior, que tenham, ou pretendam vir a ter acesso a material criptográfico, nas marcas nacionais ou estrangeiras, estabelecidas nos acordos internacionais ou bilaterais de que Portugal faça parte.

6. EXECUÇÃO

a. Princípio da Necessidade de Conhecer.

1) A "Necessidade de Conhecer" é o princípio basilar da segurança a observar no acesso à IC, de modo a garantir que a disseminação deste tipo de informação é limitada aos indivíduos que tenham uma justificada necessidade do seu conhecimento e possuam uma habilitação de segurança apropriada. O facto de se possuir uma habilitação de segurança igual ou superior ao grau da IC que se pretende aceder, não constituirá por si só autorização para tal, sendo condição necessária ter a efetiva necessidade de a conhecer.

2) O acesso a material criptográfico segue o mesmo princípio, devendo limitar-se apenas aos indivíduos que possuam uma autorização adequada, através de um CCSP nas marcas e graus de classificação de segurança do referido material e uma Autorização Cripto, bem como uma justificável necessidade de conhecer para o cabal desempenho das suas funções.

3) A nenhuma pessoa será dada autorização de acesso a material criptográfico em virtude da sua função/cargo, posto/categoria, ou posse de um CCSP para acesso a IC, a menos que possua, paralelamente a este, uma Autorização Cripto.

4) Os indivíduos autorizados a ter acesso a material criptográfico não devem divulgar essa informação a qualquer pessoa que não esteja autorizada para tal. Esta proibição permanece em vigor mesmo depois de cessarem as suas funções ou deixarem de ter acesso a material criptográfico, sendo que o incumprimento do disposto poderá configurar os crimes de violação de segredo de Estado, de espionagem ou de revelação de segredos, conforme aplicável, nos termos dos artigos 316º, 317º e 383º do Código Penal e artigos 33º, 34º e 35º do Código de Justiça Militar.

b. Responsabilidade Individual. Consiste no princípio fundamental de que um indivíduo é responsável por controlar e salvaguardar o material criptográfico confiado à sua guarda e perante a autoridade competente pela perda ou uso indevido desse material criptográfico.

c. Credenciação de Segurança.

1) As diversas entidades de natureza pública ou privada que tenham a necessidade de manusear IC são responsáveis pela autorização e elaboração dos respetivos processos de credenciação de segurança do seu pessoal para acesso a IC nos graus de MUITO SECRETO, SECRETO ou CONFIDENCIAL das diferentes marcas de classificação de segurança.

2) Todos os indivíduos, militares e civis que, para efeitos de desempenho de funções, necessitem de ter acesso a IC de grau CONFIDENCIAL ou superior, devem, obrigatoriamente, estar na posse de um CCSP emitido pela ANS, contendo a indicação da marca e grau de classificação de segurança a que terão acesso.

d. Padrões de Segurança do Pessoal para acesso a material criptográfico.

1) O material criptográfico, dada a sua natureza altamente sensível, constitui um alvo para a espionagem hostil. Existe uma panóplia de elementos que evidenciam e demonstram que os indivíduos que têm acesso a material criptográfico são os principais alvos de subversão.

2) É importante, por conseguinte, que seja dada especial atenção à seleção do pessoal destinado a atividades que requeiram Autorização Cripto, devendo prestar-se a devida atenção aos comportamentos do pessoal que possam não ser prontamente percetíveis aquando da realização do inquérito de segurança, efetuado no âmbito do processo de credenciação de segurança e que podem constituir uma potencial vulnerabilidade à segurança do material criptográfico.

3) A responsabilidade final pela segurança criptográfica cabe ao responsável máximo da organização, pelo que devem ser considerados os seguintes requisitos mínimos para efeitos de credenciação de segurança do pessoal que necessite de ter acesso a material criptográfico:

a) Pessoal encarregado de supervisionar a custódia e de custodiar o material criptográfico. Os Oficiais SEGCOM, Custódios Cripto, Custódio Cripto Substitutos e coadjuvantes devem ser credenciados no mais alto grau de classificação de segurança do material criptográfico à sua guarda. Nos órgãos de segurança criptográfica onde sejam controlados dez ou mais títulos curtos diferentes de material criptográfico com a classificação de SECRETO CRIPTO é exigido que estes elementos no âmbito da sua Autorização Cripto sejam credenciados em MUITO SECRETO CRIPTO.

b) Utilizadores de material criptográfico. Os indivíduos que no curso normal das suas funções necessitem de ter acesso regular a material criptográfico devem possuir um CCSP válido, para o mais alto grau de classificação de segurança do material criptográfico confiado à sua guarda ou a que tenham acesso e possuir a respetiva Autorização Cripto. Os utilizadores que tenham apenas necessidade de acesso a material criptográfico de grau RESERVADO devem ter sempre a necessidade de conhecer e receber um *briefing* de segurança criptográfica, a fim de serem instruídos sobre a utilização do material e da sua responsabilidade em salvaguardá-lo, incluindo os procedimentos de destruição de rotina, de evacuação e destruição de emergência.

e. Autorização Cripto.

1) O princípio da necessidade de conhecer para material criptográfico é reforçado através do uso do designador de categoria especial CRIPTO/*CRYPTO,* em complemento à classificação de segurança, para indicar que o acesso a este tipo de material é restrito a indivíduos expressamente autorizados.

2) Os indivíduos que, no desempenho normal das suas funções, necessitem de ter acesso a material criptográfico identificado com o designador de categoria especial CRIPTO/*CRYPTO*, devem possuir um CCSP em conformidade com o mais elevado grau de classificação de segurança do material criptográfico a manusear e serem especificamente autorizados pelo responsável máximo da organização ou seu representante legal, a quem compete garantir que esses indivíduos possuem qualidades de lealdade funcional, competência profissional e idoneidade cívica para terem acesso e salvaguardar todo o material criptográfico que lhes será confiado.

3) Apenas será necessária a obtenção prévia de um CCSP para os graus de classificação de segurança MUITO SECRETO CRIPTO, SECRETO CRIPTO e CONFIDENCIAL CRIPTO, tal como para os restantes diferentes tipos de marcas, tendo em consideração o âmbito do material criptográfico a manusear.

4) Deste modo, para os indivíduos a credenciar com o designador de categoria especial CRIPTO/CRYPTO (não aplicável à marca UE), deverão ser observados os seguintes requisitos:

   a) Os elementos essenciais para a atribuição de uma Autorização Cripto são os seguintes:

      (1) Os indivíduos deverão possuir um CCSP válido, de acordo com o mais elevado grau de classificação de segurança do material criptográfico a que necessitam de ter acesso regular e constante. Para obtenção do CCSP com o designador de categoria especial CRIPTO/CRYPTO, deve o pedido ser registado no Sistema de Segurança Eletrónica da Informação (SEIF), obedecendo ao que está estipulado na NT E 08, classificado em CONFIDENCIAL e ser submetido ao GNS em suporte físico. Este envio deverá ser efetuado somente após o processo de credenciação anterior necessário, conducente à obtenção do CCSP na marca e grau pretendido, conforme referido na NT E 01, ter sido submetido na plataforma de Credenciações de Segurança *Online* (CRESO).

      (2) Adicionalmente, deverá ser entregue em suporte físico a seguinte documentação classificada em CONFIDENCIAL:

         (a) Declaração de responsabilidade emitida pelo Chefe Hierárquico e validada pelo responsável máximo da organização ou seu representante legal (Anexo A), a atestar que o indivíduo a credenciar possui qualidades de lealdade funcional, competência profissional e idoneidade cívica para ter acesso a material criptográfico.

(b) Declaração de responsabilidade do próprio, validada pelo responsável máximo da organização ou seu representante legal (Anexo B), a atestar que se responsabiliza pelo cumprimento das determinações de segurança em vigor e que está perfeitamente consciente de que quando cessar as funções que determinaram o acesso a material criptográfico, continuará a estar sujeito às sanções previstas nas leis e regulamentos se, intencionalmente ou por negligência, permitir que IC de cariz criptográfico a que tiver acesso chegue ao conhecimento de pessoas não autorizadas.

(c) Informação justificativa assinada pelo Chefe Hierárquico, responsável máximo da organização ou seu representante legal (Anexo C), a atestar da necessidade de atribuição da credenciação, devido à natureza das funções a desempenhar que implicam o acesso e manuseamento de material criptográfico no grau de MUITO SECRETO CRIPTO, ou graus equivalentes de marcas de OI de que Portugal faça parte.

(d) Caso o individuo já tiver sido credenciado há mais de três meses, será necessário instruir em suporte papel um novo processo de credenciação de segurança, que deverá incluir a Ficha Individual, a Declaração de conhecimento das sanções previstas no Código Penal e no Código de Justiça Militar, bem como a respetiva Nota de Assentos (aplicável aos militares) ou Informação Disciplinar (aplicável a colaboradores civis).

(e) Os indivíduos deverão ser instruídos, através da realização de um *briefing* de segurança criptográfica, a cargo do respetivo Oficial SEGCOM ou Custódio Cripto da sua organização, de acordo com a instruções descritas no Anexo D, sobre as ameaças que pendem sobre o material criptográfico. Devem ainda ser instruídos sobre os requisitos de segurança que regulam o controlo e salvaguarda do referido material, designadamente as medidas de proteção contra perda, roubo, captura, divulgação não autorizada, observação, etc., e nos prejuízos que tais violações de segurança implicariam se pessoas não autorizadas tivessem acesso a esse mesmo material. No final do *briefing* de segurança criptográfica, todos os indivíduos devem assinar o respetivo Certificado de Autorização Cripto (Anexo D), que assumirá a forma de termo de responsabilidade, a atestar que receberam o *briefing* de segurança criptográfica e compreenderam as suas responsabilidades no que concerne ao controlo e salvaguarda do material criptográfico. O Certificado de Autorização Cripto em Anexo D deverá ser apenas utilizado para acesso a material criptográfico de índole nacional, sendo que para efeitos de acesso a material criptográfico de OI de que Portugal faça parte, deverão ser utilizados os Certificados de Autorização Cripto específicos de cada organização.

b) Todos os indivíduos detentores de "Autorização Cripto" devem receber periodicamente *briefings* de segurança criptográfica do respetivo Oficial SEGCOM ou Custódio Cripto da sua organização, isto é, a cada seis meses, com o objetivo de relembrar os aspetos abordados no *briefing* inicial. Esta ação deverá ser registada

e assinado pelo respetivo titular no verso do Certificado de Autorização Cripto (Anexo D).

c) Os CCSP e os Certificados de Autorização Cripto dos indivíduos autorizados a manusear material criptográfico devem estar disponíveis para consulta junto do Custódio Cripto da organização, ou no local onde são exercidas as funções, para fins de controlo no âmbito de ações inspetivas.

d) Quando um indivíduo, por qualquer motivo deixe de exercer as funções que deram origem à "Autorização Cripto", deverá o Oficial SEGCOM ou Custódio Cripto da organização realizar um *debriefing* de segurança criptográfica relativo às obrigações remanescentes, mesmo após a cessação da "Autorização Cripto", no qual o referido indivíduo declara, por escrito, em como se responsabiliza por não revelar qualquer IC de cariz criptográfico a pessoas não autorizadas. Esta ação será registada no respetivo Certificado de Autorização Cripto (Anexo D), devendo ser dado conhecimento desse facto à Autoridade Nacional de Distribuição (AND).

e) Sempre que um indivíduo deixe de exercer funções que impliquem o acesso a material criptográfico, por razões disciplinares ou de segurança, o responsável máximo da organização deverá apresentar à ANS, através dos canais apropriados, um relatório sobre as circunstâncias que determinaram essa medida.

f. Dispensa de Habilitação de Segurança e/ou Autorização Cripto para acesso a material criptográfico.

1) Os indivíduos detentores de um CCSP válido, que apenas tenham necessidade de acesso regular a sistemas criptográficos considerados de "baixo grau", isto é, sistemas de autenticação, códigos de utilização única ou extratos diários de listas-chave, com classificação de segurança não superior a CONFIDENCIAL, não carecem da Autorização Cripto. Excetuam-se os sistemas criptográficos igualmente considerados de "baixo grau", mas cujas instruções de utilização imponham a necessidade de uma Autorização Cripto.

2) Em situações consideradas pontuais, derivadas da necessidade operacional e por um período limitado, o responsável máximo da organização ou seu representante legal, que detém a responsabilidade de garantir a segurança física e o controlo de todo o material criptográfico a cargo da sua organização, poderá:

a) Dispensar a exigência da "Autorização Cripto" para aqueles indivíduos que possuam um CCSP válido, e que precisam de ter acesso ocasional a extratos de material criptográfico para o exercício das suas funções.

b) Renunciar a exigência do CCSP para os indivíduos que necessitem de utilizar sistemas criptográficos considerados de "baixo grau" e de classificação de segurança não superior a CONFIDENCIAL.

3) Em ambos os casos os indivíduos devem ser instruídos relativamente à utilização do material criptográfico colocado à sua disposição e sobre as responsabilidades que lhes

cabem para a salvaguardá-lo, incluindo os procedimentos de destruição de rotina, de evacuação e destruição de emergência.

g. Formação e Treino.

1) Todos os indivíduos que necessitem de ter acesso a determinado material criptográfico devem frequentar ações de formação e/ou sensibilização relativas ao controlo e salvaguarda deste tipo de material, a fim de ser garantida a sua segurança. De realçar que as quebras de segurança ou comprometimentos derivados de descuidos são menos prováveis de ocorrer se todo o pessoal estiver consciente da importância da segurança e cumprir constantemente com as regras estabelecidas. Deste modo, torna-se necessário proceder à realização de ações de formação sempre que um novo sistema ou equipamento criptográfico seja distribuído.

2) Os responsáveis por órgãos de segurança criptográfica, isto é, Oficial SEGCOM, Custódio Cripto, Custódio(s) Cripto Substituto(s), bem como o pessoal que exerça funções de operação ou manutenção de equipamentos criptográficos, devem receber treino formal, através da frequência de cursos de formação sobre a Gestão de Material Criptográfico, a ministrar pelo GNS, ou por outra entidade de reconhecida competência nesta área, designadamente o Estado-Maior-General das Forças Armadas (EMGFA) ou os Ramos das Forças Armadas. De igual modo, todos aqueles que sejam chamados a manusear material criptográfico de âmbito ESA, EU, EURATOM ou NATO, devem procurar frequentar ações de formação promovidas por estas entidades.

3) Complementarmente ao treino formal, devem ser promovidas iniciativas de treino informal para aumentar e manter a consciência de segurança dos indivíduos que manuseiam material criptográfico, através da realização de ações de sensibilização locais, formação no local de trabalho e exercícios periódicos. No âmbito dos exercícios periódicos, cuja periodicidade deverá ser semestral, será importante garantir que o pessoal é treinado e está rotinado na operação dos sistemas criptográficos detidos, mas raramente utilizados, bem como na execução de tarefas relativas aos planos de evacuação e destruição de emergência.

7. ACRÓNIMOS

a. AEE / ESA – Agência Espacial Europeia / *European Space Agency*

b. AND – Autoridade Nacional de Distribuição

c. ANS – Autoridade Nacional de Segurança

d. CCSP – Certificado de Credenciação de Segurança do Pessoal

e. CEEA / EURATOM – Comunidade Europeia da Energia Atómica / *European Atomic Energy Community*

f. CRESO – Credenciação de Segurança *Online*

g. EMGFA – Estado-Maior-General das Forças Armadas

h. GNS – Gabinete Nacional de Segurança

i. IC – Informação Classificada

j. NT – Norma Técnica

k. OI – Organizações Internacionais

l. OTAN / NATO – Organização do Tratado do Atlântico Norte / *North Atlantic Treaty Organization*

m. SEGCOM – Segurança das Comunicações

n. SEIF – Sistema de Segurança Eletrónica da Informação

o. SIC – Sistema de Informação e Comunicações

p. UE / EU – União Europeia / *European Union*

8. ANEXOS

Anexo A – Declaração de responsabilidade emitida pelo Chefe Hierárquico

Anexo B – Declaração de responsabilidade do próprio

Anexo C – Informação justificativa assinada pelo Chefe Hierárquico

Anexo D – *Briefing* e Certificado de Autorização Cripto

9. LISTA DE DISTRIBUIÇÃO

Exemplar 1 – GNS/AND

Exemplar 2 – GNS/Sub-Registo

Exemplar 3 – MNE

Exemplar 4 – EMGFA – Chefe do Gabinete do CEMGFA

Exemplar 5 – EMA

(Verso em branco)

Exemplar 6 - EME

Exemplar 7 – EMFA

Exemplar… – Outros órgãos de segurança criptográfica a constituir

(Verso em branco)

Unidade, Estabelecimento, Serviço ou Organização

Confirmo

O Comandante, Diretor ou Chefe

_____

_____

(selo branco /carimbo)

DECLARAÇÃO

(para Grau MUITO SECRETO ou equivalente)

Eu abaixo assinado, declaro que (a) , desempenhando as funções de (b) , nesta organização/serviço, é fiável e possui qualidades de lealdade funcional, competência profissional e idoneidade cívica para ter acesso a matéria classificada na MARCA (c) , no GRAU (d) e ainda que a sua reputação, conduta, hábitos e padrões de convivência constituem garantia quanto à sua discrição e capacidade de julgamento no acesso e manuseamento das informações classificadas na(s) referida(s) Marca(s) e Grau(s).

(Inserir localidade, dia, mês e ano)

O chefe hierárquico,

(Assinatura) _____

_____

(nome e posto/categoria em letras de imprensa)

(a) Posto/Categoria e nome completo
(b) Funções que desempenha
(c) MARCA pretendida (NATO, NACIONAL, UE, ESA)
(d) GRAU pretendido
NACIONAL: MUITO SECRETO CRIPTO, MUITO SECRETO
NATO: COSMIC TOP SECRET CRYPTO, COSMIC TOP SECRET
UE: TRÈS SECRET UE, (EURA TOP SECRET)
ESA: ESA TOP SECRET CRYPTO, ESA TOP SECRET

(Verso em branco)

Unidade, Estabelecimento, Serviço ou Organização

Confirmo

O Comandante, Diretor ou Chefe

_____

_____

(selo branco /carimbo)

DECLARAÇÃO

(para Grau <u>ABAIXO DE MUITO SECRETO</u> ou equivalente)

Eu abaixo assinado, declaro que (a) , desempenhando as funções de (b) , nesta organização/serviço, é fiável e possui qualidades de lealdade funcional, competência profissional e idoneidade cívica para ter acesso a matéria classificada na MARCA (c) , no GRAU (d) .

(Inserir localidade, dia, mês e ano)

O chefe hierárquico,

(Assinatura) _____

_____

(nome e posto/categoria em letras de imprensa)

(a) Posto/Categoria e nome completo
(b) Funções que desempenha
(c) MARCA pretendida (NATO, NACIONAL, UE, ESA)
(d) GRAU pretendido
NACIONAL: SECRETO CRIPTO, SECRETO, CONFIDENCIAL CRIPTO, CONFIDENCIAL
NATO: NATO SECRET CRYPTO, NATO SECRET, NATO CONFIDENTIAL CRYPTO, NATO CONFIDENTIAL
UE: SECRET UE, CONFIDENTIEL UE, (EURA-SECRET, EURA-CONFIDENTIAL)
ESA: ESA SECRET CRYPTO, ESA SECRET, ESA CONFIDENTIAL CRYPTO, CONFIDENTIAL CRYPTO

(Verso em branco)

a) Unidade, Estabelecimento, Serviço ou Organização

DECLARAÇÃO DE RESPONSABILIDADE

LEIA COM ATENCÃO AS NOTAS ABAIXO.

PREENCHA E ASSINE A DECLARAÇÃO DA PÁGINA SEGUINTE:

1. A credenciação de segurança é o ato da competência da Autoridade Nacional de Segurança, mediante o qual as pessoas são formalmente responsabilizadas em matéria de segurança, nomeadamente por imperativos decorrentes da possibilidade de acesso a matérias com os graus de classificação de segurança CONFIDENCIAL, SECRETO e MUITO SECRETO ou equivalentes;

2. A credenciação de segurança baseia-se numa atitude voluntária e consciente das pessoas por ela abrangidas e tem como pressuposto a satisfação de um conjunto de condições, entre as quais, a responsabilidade, a idoneidade, a lealdade e a discrição, cuja constatação indicia a garantia da confiança indispensável à segurança;

3. O processo de credenciação, instrumento fundamental da avaliação de segurança conduzida pela Autoridade Nacional de Segurança, tem por base a habilitação para a credenciação, a qual inclui, nomeadamente, documentação que sistematiza dados pessoais sobre os habilitandos;

4. Em conformidade com o ambiente de segurança, a avaliação de segurança integra um conjunto de procedimentos que concorrem para a decisão sobre a credenciação, entre os quais o tratamento de dados e os inquéritos de segurança;

5. Os inquéritos de segurança, que concorrem para a avaliação de segurança, são realizados pelos serviços e entidades para o efeito competentes e, tendo sempre em vista os direitos, liberdades e garantias dos cidadãos, obedecem aos princípios da necessidade, da proporcional idade e da adequação.

(Verso em branco)

a) Unidade, Estabelecimento, Serviço ou Organização

VISTO
O Comandante / Diretor / Chefe,

_____

_____

(selo branco /carimbo)

DECLARAÇÃO

Declaro que me responsabilizo pelo cumprimento das determinações de segurança estipuladas nos respetivos regulamentos e especificamente:

-Pela salvaguarda e segurança das matérias classificadas de b)

-Por não permitir, intencionalmente ou por negligência, que as informações nelas contidas cheguem ao conhecimento de pessoas não autorizadas.

Mais declaro que fico perfeitamente inteirado de que quando terminar as minhas atuais funções, apesar de já não ter acesso às referidas matérias classificadas, continuarei sujeito às sanções previstas nas leis e regulamentos se, intencionalmente ou por negligência, permitir que as informações a que tiver acesso cheguem ao conhecimento de pessoas não autorizadas.

O DECLARANTE

(Assinatura) _____

_____

(posto ou categoria)

(nome e posto/categoria em letras de imprensa)

(a) Unidade, Estabelecimento, Serviço ou Organização
(b) Indicar a MARCA e o GRAU

(Verso em branco)

Unidade, Estabelecimento, Serviço ou Organização

INFORMAÇÃO JUSTIFICATIVA

(para Grau MUITO SECRETO ou equivalente)

A necessidade de atribuição da credenciação em (a) a (b) é justificada pelo facto de o/a habilitando/a ter de desempenhar a função/cargo de (c) , a qual implica o acesso a (e o manuseamento de) matéria/informação classificada naquela(s) Marca(s) e Grau(s).

(Inserir localidade, dia, mês e ano)

O chefe hierárquico,

(Assinatura) _____

_____

(nome e posto ou categoria em letras de imprensa)

Selo branco / Carimbo

(a) Indicar a MARCA e o GRAU requerido
- NACIONAL: MUITO SECRETO CRIPTO, MUITO SECRETO
- NATO: COSMIC TOP SECRET CRYPTO, COSMIC TOP SECRET
- UE: TRÈS SECRET UE, (EURA TOP SECRET)
- ESA: ESA TOP SECRET CRYPTO, ESA TOP SECRET

(b) Identidade do habilitando (nome e posto/categoria)
(c) Indicar a natureza das funções/cargo e o local de trabalho do habilitando (que justificam o pedido neste grau)

(Verso em branco)

BRIEFING E CERTIFICADO DE AUTORIZAÇÃO CRIPTO

BRIEFING INCIAL DE AUTORIZAÇÃO CRIPTO

1. **Introdução.** Ao ser selecionado para desempenhar funções que exigem o acesso a material criptográfico, é fundamental que esteja ciente de certos factos e responsabilidades antes que esse acesso seja concedido. Este *briefing* fornece informações básicas sobre os requisitos de segurança adicionais necessários para proteger o material criptográfico e sobre os danos que podem ocorrer derivados da divulgação deste material a pessoas não autorizadas. O pessoal que necessite de Autorização Cripto deve estar na posse de um Certificado de Credenciação de Segurança ~~do~~ Pessoal (CCSP) válido e adequado ao grau de classificação de segurança do material de que necessita aceder.

2. **Necessidade de Conhecer.** O conhecimento dos sistemas criptográficos está confinado aos indivíduos com necessidade de conhecer. Nenhuma divulgação de informações relativas a tais sistemas criptográficos deverá ser feita a indivíduos ou autoridades não autorizadas a receber tais informações.

3. **Designador de Categoria Especial.** O princípio da necessidade de conhecer é reforçado pela utilização de designadores de categorias especiais, para além da classificação de segurança. Isso indica que o acesso é limitado a indivíduos autorizados. O material criptográfico ostenta o designador de categoria especial CRIPTO / *CRYPTO*.

4. **Responsabilidades.** Qualquer indivíduo que tenha na sua posse material criptográfico classificado é diretamente responsável pela sua salvaguarda e deve garantir que qualquer pessoa a quem transfira o material, está autorizada a recebê-lo. É igualmente responsável por seguir as regras de segurança em todos os momentos e por reportar quaisquer circunstâncias, ocorrências, atos intencionais ou inadvertidas que possam levar à divulgação de informação criptográfica classificada ou de material criptográfico classificado a pessoas não autorizadas. Os detalhes dos procedimentos relativos ao manuseamento de material criptográfico encontram-se detalhados em NT do GNS.

5. **Sensibilidade do material-chave.** Todo o material-chave, independentemente da sua classificação de segurança, deve ser protegido durante todo o seu ciclo de vida, desde a sua produção, até à

sua substituição e destruição. O material criptográfico que ostenta a designação CRIPTO está sujeito a controlos específicos que regem a produção, distribuição, transferência, controlo, utilização e destruição de acordo com as orientações contidas em NT do GNS. Esses controlos são projetados para garantir que o acesso ao material-chave é estritamente limitado a indivíduos que possuam um CCSP apropriado e uma Autorização Cripto.

6. **Segurança Física.** O objetivo da Segurança Física consiste em manter a integridade do material criptográfico contra o acesso não autorizado. Para garantir a segurança das comunicações classificadas é importante proteger o material criptográfico contra a perda ou o acesso não autorizado. Qualquer pessoa que tenha conhecimento ou suspeite que material criptográfico foi perdido ou possivelmente comprometido, ou ainda que qualquer informação criptográfica tenha chegado ao conhecimento de pessoas não autorizadas, deverá reportar imediatamente os factos ao Oficial SEGCOM, ou a outro individuo responsável pelo material criptográfico. Se um evento de comprometimento for revelado, devem ser tomadas medidas imediatas para limitar a quantidade de informação perdida. Se o comprometimento não for revelado, os utilizadores presumem que a sua segurança se mantém intacta, continuando a transmitir informação através do sistema comprometido. É por estas razões que a notificação imediata de quaisquer incidentes suspeitos é tão importante.

7. Após a realização deste *briefing*, deve assinar uma cópia do Certificado de Autorização Cripto, declarando que compreendeu o seu conteúdo e está ciente dos danos envolvidos na divulgação intencional ou inadvertida de informação criptográfica a qualquer pessoa não autorizada. Este formulário autoriza que tenha acesso a informação criptográfica até a classificação de segurança indicada. Não lhe dá o direito a aceder a informação criptográfica para a qual não tenha necessidade de conhecer, nem lhe dá o direito a entrar numa instalação criptográfica, a menos que as suas funções exijam a sua presença.

DEBRIEFING DE CESSAÇÃO DE AUTORIZAÇÃO CRIPTO

1. Não necessita mais de aceder a material criptográfico. Durante o período em que teve acesso foi informado através de *briefings* e refrescamentos periódicos relativos às responsabilidades decorrentes da Autorização Cripto, que a informação de que tomou conhecimento através do acesso ao material criptográfico, nunca deverá, em circunstância alguma, ser divulgada a pessoas não autorizadas.

2. É relembrado que os itens que ostentam o designador de categoria especial CRIPTO são especialmente sensíveis, porque são utilizados para proteger outra informação classificada contra o acesso não autorizado. Se a integridade de um sistema criptográfico for comprometida em qualquer momento, durante a sua existência, toda a informação classificada protegida por esse sistema, ao longo do seu ciclo de vida, poderá ser comprometida.

3. Por conseguinte, a aplicação estrita do princípio da necessidade de conhecer continua a ser essencial, mesmo agora que já não tem um requisito para acesso ao material criptográfico.

4. Independentemente do facto de estar a ser submetido a um *Debriefing* de Cessação de Autorização Cripto e de já não ter necessidade de aceder a material criptográfico, deve reportar imediatamente ao responsável máximo da organização e ao Oficial SEGCOM, de qualquer quebra de segurança ou comprometimento, do qual tome conhecimento. Será da responsabilidade do responsável máximo da organização e/ou Oficial SEGCOM garantir que a Autoridade Nacional de Distribuição é imediatamente informada.

5. Deve assinar a Parte 2 do Certificado de Autorização Cripto, em como declara que compreendeu o *Debriefing* de Cessação de Autorização Cripto e que os dados pessoais que constam do certificado estão corretos. Uma cópia do Certificado de Autorização Cripto, registando o seu *Briefing* Inicial de Autorização Cripto e o *Debriefing* de Cessação de Autorização Cripto, será mantida pelo Custódio Cripto.

CERTIFICADO DE AUTORIZAÇÃO CRIPTO

PARTE I – *BRIEFING* INICIAL		
NOME:	POSTO:	ESPECIALIDADE / ARMA:
CREDENCIAÇÃO DE SEGURANÇA:	CLASSIFICAÇÃO DE SEGURANÇA DO MATERIAL E/OU INFORMAÇÃO CRIPTOGRÁFICA PARA O QUAL O ACESSO É AUTORIZADO:	
CARGO/DESCRIÇÃO DE FUNÇÕES:		
DECLARAÇÃO DE RESPONSABILIDADE: Eu,_____, declaro, por este meio, que recebi um *briefing* de Segurança Criptográfica do (indicar o Órgão de Segurança Criptográfica do qual recebeu o *briefing*). Eu compreendo que a segurança do material criptográfico e da informação criptográfica é de extrema importância e que a sua perda ou comprometimento pode conduzir a consequências graves para a segurança da Nação. Fui instruído sobre os requisitos de segurança relativos à divulgação de informação relacionada com material criptográfico. Compreendo os requisitos de segurança que regulam o controlo e salvaguarda do material criptográfico, para o qual estou a obter autorização de acesso.		
ASSINATURA DA PESSOA AUTORIZADA:		
DATA:		
ASSINATURA DA ENTIDADE QUE AUTORIZA:		
DATA:	FUNÇÕES:	
PARTE II – *DEBRIEFING* DE CESSAÇÃO DE AUTORIZAÇÃO CRIPTO		
CONFIRMAÇÃO DE RESPONSABILIDADE: Eu,_____, declaro, por este meio, que recebi um *debriefing* de Segurança Criptográfica ao deixar as minhas funções. É do meu inteiro conhecimento a importância para a segurança da Nação da continuação da salvaguarda da informação criptográfica, assim como é do meu conhecimento que me encontro ainda abrangido pela legislação e regulamentos de segurança nacional, respeitantes à revelação não autorizada de informação criptográfica.		
ASSINATURA DA PESSOA AUTORIZADA:		
DATA:		
ASSINATURA DO OFICIAL SEGCOM:		
DATA:		

(Verso em branco)

BRIEFINGS	DATA	ASSINATURA	RESPONSÁVEL
INICIAL			
PRIMEIRO SEMESTRAL			
SEGUNDO SEMESTRAL			
TERCEIRO SEMESTRAL			
QUARTO SEMESTRAL			
QUINTO SEMESTRAL			
SEXTO SEMESTRAL			
SÉTIMO SEMESTRAL			
OITAVO SEMESTRAL			
NONO SEMESTRAL			
DÉCIMO SEMESTRAL			