Este folheto sintetiza alguns conceitos e medidas de segurança aplicáveis a documentos classificados em conformidade com as Regras de Segurança e políticas de Informação Classificada (Nacional, UE, NATO). O seu conteúdo é puramente indicativo e não substitui nem os conceitos das próprias Regras de Segurança, nem as políticas ou diretrizes de segurança para a sua execução

1. O que é Informação Classificada (IC)? (SEGNAC 1 – Anexo A (Glossário de termos))

Informação cuja divulgação não autorizada pode causar prejuízos aos interesses do Estado ou de um Estado-Membro de uma Organização Internacional (OI), da qual Portugal faça parte.

Estes prejuízos são graduados como DESFAVORÁVEIS, PREJUDICIAIS, GRAVES ou EXTRAORDINARIAMENTE GRAVES, a que correspondem os graus da IC RESERVADO, CONFIDENCIAL, SECRETO ou MUITO SECRETO, respetivamente.

2. Quais as Marcas e Graus da IC?

A IC pode ter Marca Nacional ou de uma OI (Ex.: OTAN/NATO - Organização do Tratado do Atlântico Norte; EU/UE - União Europeia; ESA - Agência Espacial Europeia).

Marca	Nacional	OTAN/NATO	EU/EU	ESA
Grau	MUITO SECRETO	COSMIC TOP SECRET	TRES SECRET UE/EU TOP SECRET	TRES SECRET ESA/ESA TOP SECRET
	SECRETO	NATO SECRET	SECRET UE/EU SECRET	SECRET ESA/ESA SECRET
	CONFIDENCIAL	NATO CONFIDENTIAL	CONFIDENTIEL UE/EU CONFIDENTIAL	CONFIDENTIEL ESA/ESA CONFIDENTIAL
	RESERVADO	NATO RESTRICTED	RESTREINT EU/ EU RESTRICTED	RESTREINT ESA/ESA RESTRICTED

3. O que é, para que serve e quem atribui uma Credenciação de Segurança?

É uma habilitação de uma pessoa, singular ou coletiva, para manusear IC, atribuída pela Autoridade Nacional de Segurança (ANS).

4. Quem necessita de Credenciação de Segurança? (SEGNAC 1 – cap.4)

Todos que necessitem de aceder a IC de grau igual ou superior a CONFIDENCIAL;

NOTA: Os Membros do Governo da República Portuguesa e dos Governos Regionais são credenciados por inerência de funções.

5. Como se processa o pedido de Credenciação?

Na página do GNS (https://www.gns.gov.pt), em Credenciações de Segurança (CRESO).

6. Qual o significado e características das Áreas de Segurança? (SEGNAC 1 – cap.5.3)

São locais formalmente designados como tal, cujas condições de segurança respeitam critérios relacionados com o grau da IC neles manuseada/guardada e com a forma como é trabalhada, identificados como: Área Administrativa ou Área de Segurança Classe 3 (ASC3), Área de Segurança Classe 2 (ASC2) e Área de Segurança Classe 1 (ASC1).

	Área Administrativa ou ASC 3	ASC 2	ASC 1
Máx. Grau	Até RESERVADO	Até MUITO SECRETO	Até MUITO SECRETO
Caraterísticas	Sem requisitos especiais de segurança.	Locais onde assuntos classificados são trabalhados, manuseados e guardados temporariamente (não arquivados)	Áreas muito sensíveis em que o acesso equivale ter acesso à IC.
Medidas	Acesso controlado ao edifício.	Acesso controlado ao edifício. Controlos internos que impeçam o acesso à área, de pessoas não autorizadas.	Acesso controlado ao edifício. Obrigatório controlo de acessos à área com registo individual.
Exemplos	Zonas de circulação ou locais de acesso não condicionado.	Gabinetes de trabalho, salas de reunião.	Sub-Registos, Postos de controlo, Centros de Dados, Salas de Situação, Centros de Operações.

Nota: Estas situações não dispensam a consulta das normas aplicáveis.

7. Como guardar a IC? (SEGNAC 1 – cap.5.3 e 5.6)

	RESERVADO	CONFIDENCIAL	SECRETO	MUITO SECRETO
Área de Segurança	Área Administrativa ou ASC 3	ASC 1 e ASC 2	ASC 1 e ASC 2	ASC 1
Exemplos	Móvel escritório c/chave	Armário metálico c/ tranca e cadeado (4 combinações)	Cofre	Casa-Forte ou cofre

8. Quais os procedimentos a ter no manuseamento da IC em suportes digitais e em infraestruturas de redes?

A tramitação digital da IC dos graus RESERVADO, CONFIDENCIAL ou SECRETO, só é permitida usando produtos ou mecanismos criptográficos certificados e acreditados pela ANS.

9. Como pode copiar, transferir, reproduzir e/ou destruir IC?

A IC de grau igual ou superior a CONFIDENCIAL só pode ser copiada, transferida, reproduzida e/ou destruída por um Sub-Registo ou Posto de Controlo;

Cada cópia de um documento classificado é um documento com registo próprio que obriga a um controlo específico.

10. O que é uma quebra de segurança e/ou comprometimento de segurança? (SEGNAC1, cap.9)

Quebra de segurança - Atos ou omissões que violem as regras de segurança estabelecidas e que façam perigar ou comprometer a IC.

Comprometimento – Acesso a IC, parcial ou total, por pessoa não autorizada.

11. Como proceder em caso de comprometimento de IC ou quebra de segurança? (SEGNAC1, cap.9)

- Comunicar imediatamente às autoridades competentes;
- Informar, paralelamente, a entidade que originou o documento que continha as informações comprometidas;
  Obs: A urgência desta comunicação dependerá das circunstâncias conjunturais e do grau de classificação da informação em causa;
- Comunicação imediata à ANS sempre que:
  - se trate de IC de Grau MUITO SECRETO;
  - haja indícios ou suspeitas de espionagem.

12. Quais os cuidados para evitar comprometimento de IC e/ou quebra de segurança? (SEGNAC1, cap.7.3)

- Manusear IC, somente, em áreas de segurança e com equipamentos certificados e acreditados pela ANS;
- Não reproduzir ou digitalizar IC sem o controlo do Sub-Registo ou Posto de Controlo;
- Não levar IC para fora das instalações;
- Não ter conversas sobre IC em locais não seguros e/ou na presença de pessoas sem necessidade de conhecer e sem a credenciação adequada. (ex.: restaurantes, aeroportos, transportes, hotéis, etc.);
- Não usar a rede telefónica e/ou internet para troca de IC;
- Não usar equipamentos que captem som e imagem (ex.: telemóvel, câmara fotográfica) em áreas de segurança de Classe 1 ou 2.

13. O que é o "Dever de Sigilo"?

Consiste em guardar segredo profissional relativamente a informação de que tenha conhecimento em virtude do exercício das suas funções e que não se destinem a ser do domínio público.

14. Procedimentos recomendados na cessação de funções

- Receber o *debriefing* de segurança do Chefe do Sub-Registo ou do Encarregado de Segurança;
- Assinar um Termo de Responsabilidade de cessação de funções comprometendo-se ao dever de sigilo;
- Entregar toda a IC que esteja em sua posse e cartões de acesso às áreas de segurança ao Chefe do Sub-Registo ou ao Encarregado de Segurança;
- Solicitar ao Departamento de Informática o cancelamento do acesso ao email e às pastas de trabalho em rede.

Para aceder a mais documentação, consulte o nosso website: www.gns.gov.pt
Para obter mais conhecimentos: Curso de Introdução à Segurança da Informação Classificada
https://www.nau.edu.pt/pt/curso/introducao-a-seguranca-da-informacao-classificada/
Para esclarecimento de dúvidas envie-nos um email: formacao@gns.gov.pt ou telefone: +351 210403616

2024 V. 4.2