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)?

Informações ou material, com uma classificação de segurança, 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.

2. Quais as Marcas e Graus da IC?

A IC pode ter a Marca Nacional ou de uma OI, das quais se destacam a União Europeia (EU/UE) e a Organização do Tratado do Atlântico Norte (OTAN/NATO).

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

3. Para que serve uma Credenciação de Segurança e quem a atribui?

Habilita uma pessoa singular ou coletiva a manusear IC, sendo atribuída pela Autoridade Nacional de Segurança (ANS).

4. Quem precisa de estar credenciado?

Todas as pessoas que tenham necessidade de aceder a IC de Grau igual ou superior a CONFIDENCIAL.

5. Como se processa o pedido de Credenciação?

Na página do GNS, em Credenciações de Segurança (CRESO), encontra todos os serviços relativos aos pedidos de credenciações de segurança por cidadãos, empresas e entidades públicas. Em situações excecionais poderá ser atribuída uma credenciação temporária pela ANS.

6. Qual o significado das Áreas de Segurança de CLASSE 1, 2 ou 3?

CLASSE 1 - Área onde pode ser manuseada e guardada a IC de Grau CONFIDENCIAL, SECRETO e MUITO SECRETO, sendo obrigatório o registo e o controlo de acessos. (p.ex. Posto de Controlo, Sub-registo, Centro de Dados, Salas de Situação);

CLASSE 2 – Área onde pode ser manuseada a IC de Grau CONFIDENCIAL, SECRETO e MUITO SECRETO e guardada somente a de Grau CONFIDENCIAL, sendo obrigatório o controlo de acessos (p.ex. Gabinetes da Direção e Salas de trabalho);

CLASSE 3 ou **Área Administrativa** - Só pode ser manuseada e guardada a IC de Grau RESERVADO e não necessita de controlo de acessos (p.ex. áreas de circulação ou de acesso não condicionado).

7. Como guardar a IC?

RESERVADO	CONFIDENCIAL	SECRETO	MUITO SECRETO
Área Administrativa e Móvel escritório c/chave	Área Classe 1 ou 2 e Armário metálico c/ tranca e cadeado (4 combinações)	Área Classe 1 ou 2 e Armário tipo Cofre	Área Classe 1 e Cofre ou Casa - Forte

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

Utilizar somente Sistemas de Informação e de Comunicações (SIC) que sejam acreditados e autorizados pela ANS. Apenas é permitido o envio de IC através sistemas não autorizados pela ANS (p. ex: email) desde que cifrada e na Marca Nacional até ao Grau Reservado.

Gabinete Nacional de Segurança

Rua da Junqueira, 69, 1300-342 Lisboa | Tel (+351) 21 303 17 10 | Fax (+351) 21 303 17 11 | geral@gns.gov.pt

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

Para Grau igual ou superior a CONFIDENCIAL, apenas através do Órgão de Segurança (Posto de Controlo ou Sub-registo). Cada cópia passa a constituir um exemplar com registo próprio.

10. O que é um comprometimento de segurança e/ou quebra de segurança?

O comprometimento implica o conhecimento parcial ou total de IC, por parte de pessoas não autorizadas.
A quebra resulta de atos ou omissões que violem as regras de segurança estabelecidas e que façam perigar ou comprometer a IC.

11. Quais os cuidados elementares para evitar um comprometimento e/ou quebra de segurança?

Manusear somente IC em áreas e com equipamentos acreditados.

Só são permitidas conversas sobre IC na presença de pessoas com necessidade de conhecer, para além de possuírem a credenciação adequada.

Não discutir IC em espaços públicos onde possa ser ouvido (p.ex. cafés, restaurantes, aeroportos, transportes, hotéis). Assuma que um telefone está sujeito a monitorização externa e não tenha conversações telefónicas sobre IC.

É proibido o uso de dispositivos eletrônicos pessoais que captem sons e imagens (p.e.: smartphone, tablet, câmara fotográfica, etc…) em qualquer sala onde se realiza a consulta e o manuseamento de IC.

Nenhuma IC de Grau superior ou igual a CONFIDENCIAL pode ser levada para fora das instalações em que se encontra depositada com a finalidade de ser trabalhado em casa ou por quaisquer outras razões. No que se refere a IC de Grau RESERVADO, poderá ser levada para fora das instalações, com conhecimento do chefe direto, que registará sempre, de forma bem clara, a saída da IC.

Os funcionários não são autorizados a fotocopiar ou digitalizar documentos, contendo IC de Grau igual ou superior a CONFIDENCIAL nem possuir arquivos particulares ou registos dessa documentação.

12. Como proceder em caso de comprometimento ou quebra de segurança?

Deverá o facto ser imediatamente comunicado às autoridades competentes, segundo os Canais normais.
A entidade que comunica deverá informar, paralelamente, a entidade que emitiu o documento que continha as informações comprometidas. A urgência desta comunicação dependerá das circunstâncias conjunturais e do grau de confidencialidade da informação em causa.
Deve ser feita imediatamente uma comunicação à ANS sempre que:
- se trate de IC de Grau MUITO SECRETO;
- haja indícios ou suspeitas de espionagem.

13. O que é o "Dever de Sigilo"?

Preservar para si o conhecimento obtido durante e após o termo do exercício de funções, onde lhe foi conferido acesso a IC.

14. <u>Procedimentos a ter quando da cessação de funções</u>

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

Em caso de dúvida, envie-nos um *email* (formacao@gns.gov.pt) ou telefone (+351210403616) que nós esclarecemos. Para aceder a mais documentação, consulte o nosso *website*: www.gns.gov.pt