NT – B 02
29JUL2024

NORMA TÉCNICA – B 02

REQUISITOS MINIMOS DE SEGURANÇA A OBSERVAR POR SISTEMAS DE INFORMAÇÃO E DE COMUNICAÇÃO (SIC) QUE PRODUZEM, ARQUIVAM, PROCESSAM OU DISSEMINAM INFORMAÇÃO CLASSIFICADA (IC)

Lisboa, 29 de julho de 2024

A Autoridade Nacional de Segurança

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2024.07.25 21:19:32 +01'00'

(António Gameiro Marques)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

1. REFERÊNCIAS

a. Nacionais:

1) Lei Orgânica do GNS, Decreto-Lei nº3/2012, de 16 de janeiro, na sua atual redação;
2) Resolução do Conselho de Ministros nº 50/88, de 3 de dezembro (SEGNAC 1);
3) Resolução do Conselho de Ministros nº 37/89, de 24 de outubro (SEGNAC 2);
4) Resolução do Conselho de Ministros nº 16/94, de 22 de março (SEGNAC 3);
5) Resolução do Conselho de Ministros nº 05/90, de 28 de fevereiro (SEGNAC 4).

b. Organização do Tratado do Atlântico Norte (OTAN/NATO):

1) C-M(2002)49 *NATO Security Policy*;
2) AC/35-D/2004 – *Primary Directive on CIS Security*;
3) AC/35-D/2005 – *Management Directive on CIS Security*;
4) AC/35-D/1021 – *Guidelines for the Security Accreditation of CIS*;
5) AC/35-D/1017 – *Guidelines for the Security Risk Management of CIS*;
6) AC/35-D/1015 – *Guidelines for the Development of Security Requirements Statements* (SRSs);
7) AC/35-D/1014 – *Guidelines for the Structure and Content of Security Operating Procedures* (SecOps) for *CIS*;
8) AC/35-D/1039 – *Guidelines on Business Continuity Planning for CIS*;
9) AC/35-D/2001 - *Directive on Physical Security*;
10) AC/35-D/1050 & AC/322-D(2019)0001 – *Supporting Document for the protection of NATO information within Public Cloud-based Communication and Information Systems (CIS);*
11) AC/322-D/0047 - *Technical and Implementation Directive on Cryptographic Security and Cryptographic Mechanisms*;
12) AC/322-D/0048 - *Technical and Implementation Directive on CIS Security*;
13) AC/322-D/0049 - *Technical and Implementation Directive for Transmission Security*;
14) AC/322-D(2007)0036 - *Technical and Implementation Directive on Emission Security*;
15) AC/322-D/0030 - *Technical and Implementation Directive for the Interconnection of CIS*.

c. União Europeia:

1) DECISÃO DO CONSELHO de 23 de setembro de 2013 relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE);
2) DECISÃO (UE, EURATOM) 2015/444 DA COMISSÃO de 13 de março de 2015 relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE;
3) DECISÃO (UE, EURATOM) 2017/46 DA COMISSÃO de 10 de janeiro de 2017 relativa à segurança dos sistemas de comunicação e de informação na Comissão Europeia;
4) *Information Assurance (IA) Security Policy on Security Throughout the CIS Life Cycle – IASP-L*;

5) *IA Security Policy on Security Governance – IASP-G*;
6) *IA Security Policy on Risk Management – IASP 1*;
7) *IA Security Policy on Cryptography – IASP 2*;
8) *IA Security Policy on Interconnection – IASP 3*;
9) *IA Security Policy on Network Defence – IASP 4*;
10) *IA Security Policy on CIS Security Engineering – IASP 5*;
11) *IA Security Policy on Qualification and Approval of non-cryptographic Products – IASP 6*;
12) *IA Security Policy on TEMPEST – IASP 7*;

d. Outras:

1) SDIP 27 – *NATO TEMPEST Requirements and Evaluation Procedures*;
2) SDIP 28 – *NATO Zoning Procedures*;
3) SDIP 29 - *Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information*;
4) Quadro Nacional de Referência para a Cibersegurança (QNRCS);
5) ISO/IEC 21827:2008 *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model®* (SSE-CMM®).

2. DEFINIÇÕES

a. Avaliação de Segurança:[1] Aferição imparcial feita sobre um produto, sistema ou serviço, por um órgão independente, visando fornecer aos potenciais consumidores de tais produtos, a confiança nas funcionalidades e mecanismos de segurança implementados, assim como, uma métrica para comparar os diferentes recursos de segurança de cada produto. Ao produto ou SIC sujeito a avaliação dá-se o nome de *Target of Evaluation* (TOE).

b. Certificação de Segurança:[2] Procedimento pelo qual uma entidade atesta que um produto, sistema ou serviço, depois de avaliado, está em conformidade com os requisitos de segurança pré-definidos para uma dada marca e grau. Incide sobre os fabricantes e produtores de produtos, equipamentos ou serviços usados no manuseamento de Informação Classificada (IC).

[1] Tradução livre do documento "*GUIDELINES for the SECURITY EVALUATION and CERTIFICATION of communication and information systems* (CIS) - AC/35-D/1019-REV1"
[2] Idem

c. **Acreditação de Segurança:**[3] Autorização formal para a exploração de um dado sistema, emitida pela Autoridade Nacional de Segurança, com base no resultado de um processo de avaliação, tendo em vista um dado propósito, como seja, o processamento de informação classificada. Incide sobre as entidades produtoras, consumidoras e disseminadoras de IC.

d. **Sistemas de Informação (SI)[4]:** Conjunto de componentes (hardware e software) inter-relacionados que trabalham em conjunto para recolher, processar, armazenar e distribuir informação para suporte da tomada de decisão, coordenação, controlo, análise e visualização numa organização.

e. **Sistemas de Informação e de Comunicação (SIC)[5]:** Designam um qualquer sistema de informação e de comunicações que permite a produção, arquivo, o processamento e a disseminação de informação em formato eletrónico, compreendendo todos os ativos necessários para seu funcionamento, incluindo a infraestrutura, a organização, o pessoal e os sistemas de informação (SI).

f. **Componente de proteção de fronteiras (BPC)[6]:** Um componente de um sistema que fornece um serviço de proteção de fronteiras (BPS), podendo ser composto por: *firewalls*, *data diodes*, *data guards*, *routers* de filtragem, servidores *proxy*, detetores de intrusão e *software* de verificação de conteúdos de uma interligação.

g. **Serviço de proteção de fronteiras (BPS)[7]:** Um serviço de segurança que medeia os fluxos de informação ou atenua os riscos de segurança introduzidos por uma interligação de um ou mais SIC. Por exemplo, autenticação de entidades, controlo do acesso, verificação de pacotes, *anti-malware*, etc.

h. ***High Assurance Guard* (HAG)[8]:** Dispositivo de proteção de fronteira, composto por *hardware* e *software*, concebido para aplicar um conjunto de regras de segurança que controlam o acesso a informação entre uma rede local e uma rede externa com um elevado grau de confiança.

---

[3] Tradução livre do documento "*GUIDELINES for the SECURITY ACCREDITATION of communication and information systems* (CIS) - AC/35-D/1021-REV3"
[4] Tradução livre de *LAUDON, K. e LAUDON, J., Essentials of Management Information Systems, Organization and Technology, 2nd edition, Prentice-Hall*, 1996
[5] DECISÃO DO CONSELHO (2013/488/UE) de 23 de setembro relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013D0488, consultado a 08/03/2024;
[6] Tradução livre de AC/322-D/0030-REV6 - *Technical and Implementation Directive For The Interconnection Of Communications and Information Systems (CIS)*;
[7] Idem;
[8] Idem;

3. CONCEITOS

a. **Conceito de "*Security by Design*"[9]**: Abordagem de segurança sobre um produto TIC desde a sua conceção, procurando projetar padrões de segurança de forma holística, criativa, proactiva, interdisciplinar, robusta, responsável e integrada no desenho da arquitetura. É tida como o oposto de "segurança através da obscuridade".

a. **Conceito de "*Security by Default*"[10]**: Abordagem à configuração de produtos, serviços ou processos TIC, que garante a utilização por defeito de uma configuração segura, mesmo não sendo a mais fácil de utilizar, podendo ser definidas por normas ou referenciais extraídos de uma Análise do Risco e/ou de Testes de Verificação.

b. **Conceito de Informação Classificada (IC):** qualquer informação, material ou documento, independentemente da sua forma, natureza e meios de transmissão, à qual tenha sido atribuída uma marca ou um grau de classificação de segurança e que requeira proteção contra divulgação não autorizada que seja suscetível de causar dano aos interesses fundamentais do Estado, como tal definido no nº 6 do artigo 316º do Código Penal, às organizações internacionais de que Portugal faça parte ou de Estados com os quais tenha celebrado acordos internacionais para a proteção mútua da informação classificada;

c. **Conceito de Requisitos de Segurança:**[11] declaração de uma funcionalidade de segurança necessária para garantir que um dos objetivos de segurança seja satisfeito. Os requisitos de segurança, são derivados de padrões da indústria, de leis aplicáveis à segurança e de histórico de vulnerabilidades anteriores, fornecendo uma base de funcionalidades de segurança que um dado SI, deve possuir.

d. **Conceito de Controlo de Segurança:** [12] são contramedidas ou salvaguardas implementadas para evitar, detetar, neutralizar ou minimizar o risco identificado dentro do apetite e da tolerância ao risco definido pela organização. Os controlos classificam-se em deteção, prevenção ou corretivos, existindo diferentes tipos, como sejam: legais, administrativos, técnicos, procedimentais ou físicos, podendo caracterizar-se quanto à implementação como sendo automáticos ou manuais.

---

[9] Tradução livre de *Cavoukian, A., Dixon*, M. (2013). "*Privacy and Security by Design: An Enterprise Architecture Approach.*", *Oracle Corporation*, disponível em: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf, consultada em 17/08/2020;

[10] REGULAMENTO (UE) 2019/881 DO PARLAMENTO EUROPEU E DO CONSELHO de 17 de abril de 2019 relativo à ENISA (Agência da União Europeia para a cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação, consultado a 08/03/2024;

[11] Tradução livre de: https://owasp.org/www-project-proactive-controls/v3/en/c1-security-requirements, consultado em 10/07/2023;

[12]Tradução livre de: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/what-is-the-difference-between-requirements-and-controls consultado em 10/07/2023;

e. **Conceito de SIC Nacional:** são considerados como SIC nacionais todos os sistemas instalados em Portugal que utilizem chaves criptográficas nacionais, cujo acesso seja gerido por uma entidade nacional e que processem informação classificada na marca NACIONAL.

f. **Conceito de Maturidade:**[13] dá conta do grau de detalhe pelo qual um processo é explicitamente definido, gerido, aferido, controlado e capaz responder aos requisitos da organização. O conceito de maturidade implica um potencial de crescimento da capacidade organizacional e indica a riqueza e a consistência dos múltiplos processos organizacionais.

g. **Conceito de Capacidade:**[14] dá conta da probabilidade de uma organização atingir os objetivos de segurança, tendo em conta os processos internos implementados. O conceito de capacidade é gradativo e implica a existência de um processo interno de aferição do risco que possibilite identificar os requisitos que uma organização deve implementar.

h. **Conceito de Interligação**:[15] capacidade que permite a troca de informação entre dois SIC através de uma ligação estabelecida.

4. SITUAÇÃO

a. A crescente proliferação de ameaças torna essencial acautelar a correta implementação de um SIC, nivelando o risco residual dentro de um patamar aceitável por todas as partes envolvidas no processo de Acreditação de Segurança.

b. É neste sentido que a utilização de um SIC *per si* deve pressupor desde logo um nível mínimo de maturidade e o cumprimento integral de um conjunto de requisitos de segurança assentes nos conceitos *Security by Design* e *Security by Default*.

c. Aos quais deve acrescer, quando necessário, um conjunto adicional de controlos de segurança, em particular quando os desvios identificados requeiram a adoção de uma postura de segurança mais adequada ao nível de risco e ao ambiente em questão.

d. O panorama atual dá ainda conta de uma crescente competição por recursos e uma cada vez mais débil capacidade de cada organização atingir os seus objetivos, criando cada vez mais brechas na maturidade organizacional e na aptidão para definir, gerir e controlar os processos internos.

---

[13] ISO/IEC 21827 *Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model®* (SSE-CMM®)
[14] Idem
[15] Tradução livre de AC/322-D/0030-REV6 - *Technical and Implementation Directive For The Interconnection Of Communications and Information Systems (CIS)*

e. E de uma necessidade crescente por tratar um cada vez maior leque de informação classificada, sendo na maioria dos casos de diferentes marcas e graus, num dado SIC.

f. A documentação em referência estabelece não só os critérios a seguir para a acreditação de segurança de SIC, mas também um referencial de requisitos que formam um puzzle por vezes difícil de acompanhar e que se juntam com o sentido de ajudar a desenhar e utilizar um sistema de informação e de comunicação de forma segura e confiável.

5. OBJECTO/FINALIDADE

O presente documento tem como objetivo definir os requisitos mínimos de segurança a observar pelos SIC habilitadas a processar informação classificada na marca NACIONAL.

Adicionalmente, procura-se definir o conceito de sistema nacional por oposição a um sistema gerido e/ou mantido por outras entidades internacionais, procurando-se apoiar o processo de acreditação de segurança de um sistema de informação e de comunicação.

6. ÂMBITO

A presente norma destina-se a ser implementada por:

a. Entidades e organismos públicos e privados que processam informação classificada da marca NACIONAL de qualquer grau;

b. Chefes de Sub-Registo e Postos de Controlo, Responsáveis pela Segurança dos Serviços, Órgãos ou Organismos públicos, quer dentro, quer fora do país que necessitem planear, desenhar, implementar e explorar SIC para manuseio de informação classificada, independentemente do regime normativo ao qual a informação está subjacente.

7. OBJECTIVOS DA SEGURANÇA DA INFORMAÇÃO

São objetivos da segurança da informação:

a. **A confidencialidade** como atributo da IC que impede a sua divulgação a pessoas ou entidades não autorizadas ou por processos não autorizados;

b. **A integridade** como a propriedade de salvaguardar o caráter exato e completo da IC e dos ativos;

c. **A disponibilidade** como a propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada;

d. **A autenticidade** enquanto garantia de que a informação é genuína e provém de fonte fidedigna;

e. **O não-repúdio** como a aptidão de demonstrar que um ato ou acontecimento teve lugar, de modo que esse acontecimento ou ato não possa ser subsequentemente negado.

8. OBJECTIVOS DA SEGURANÇA DA INFORMAÇÃO

São princípios da segurança da informação.

a. **Análise do Risco (*Security Risk Assessment*):** Todas as TIC devem ser sujeitas a uma análise do risco e possuir ao longo de todo o ciclo de vida, um processo continuo de monitorização por forma a reduzir, eliminar, evitar ou aceitar riscos;

b. **Necessidade de conhecer (*Need-to-Know*):** através do qual apenas possui acesso a áreas e a informação classificada quem tiver real necessidade de o fazer, para o desempenho das suas funções, e que para tal possua a credenciação de segurança adequada;

c. **Simplificação (*Minimality*):** através da utilização de apenas as aplicações, os protocolos e os serviços necessários para realizar a missão operacional;

d. **Defesa em Profundidade (*Defence-in-depth*):** através da aplicação de mecanismos e controlos de segurança que promovam a proteção das TIC em exploração;

e. **Privilégios mínimos (*Least Privilege*):** Os utilizadores apenas possuem os privilégios e as autorizações necessárias para executar as suas tarefas e deveres;

f. **Auto-Proteção (*Self-protecting CIS*):** por forma a estabelecer uma linha de comando e controlo sobre os SI utilizados para a exploração de IC. Neste sentido, cada SI tratará outro SI como não confiável e deverá implementar os mecanismos de segurança necessárias para controlar a troca de informação entre SI;

g. **Postura de segurança (*Up-to-date Security Posture*):** A postura de segurança deverá ter em conta a operação, a atualização e a manutenção das TIC, devendo ser periodicamente revista por forma a manter o nível de segurança necessário para o contexto de operação;

h. **Controlo da configuração (*Configuration Management*):** deve ser utilizada uma configuração de base segura em todas as TIC, por forma a obter o nível de segurança necessário para lidar com as alterações no ambiente operacional de em função da análise do risco;

i. **Resiliência (*Resilience*):** Cada TIC deve dotar cada elemento com a agilidade suficiente e a capacidade para rapidamente se adaptar e recuperar de qualquer tipo de limitação, permitindo continuar a operar num nível aceitável de serviço;

j. **Avaliação dos requisitos de segurança (*Security Auditing Assurance*):** os requisitos de segurança devem ser avaliados e auditados por uma entidade qualificada por forma a garantir a proteção dos SIC autorizadas a manusear IC.

9. TIPOLOGIA E CONFIGURAÇÕES DE UM SIC

a. Os requisitos mínimos de segurança aplicam-se a diferentes plataformas, designadamente:

Fig.1 – Tipos de sistemas aos quais se aplicam os requisitos de segurança.

b. Assim como, a diferentes configurações de SIC, designadamente:

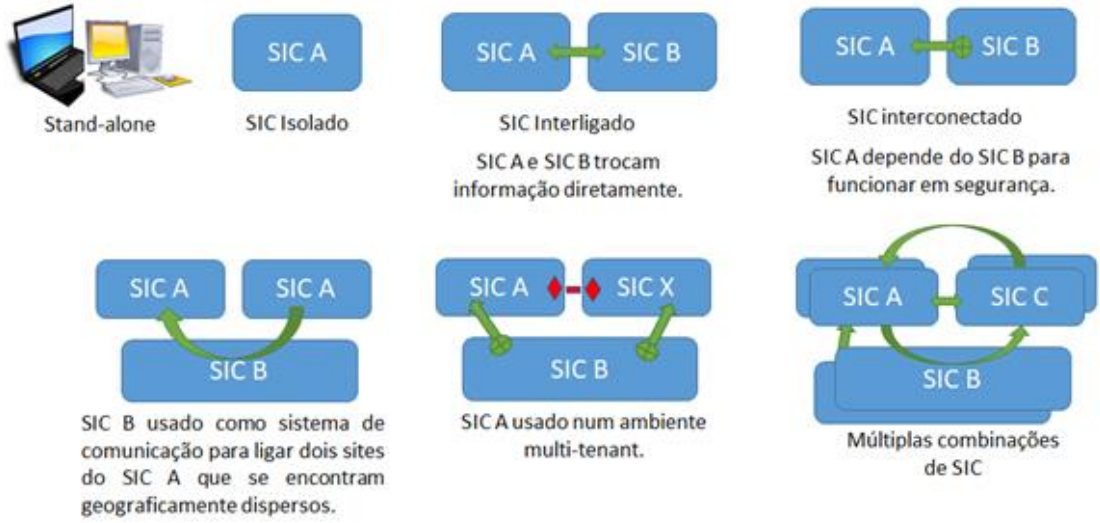

Fig.2 – Configurações de SIC aos quais se aplicam os requisitos de segurança.

c. Os processos de acreditação de segurança regem-se pela NT-B01, devendo para cada grau e arquitetura serem observados os requisitos de segurança explicitados neste documento.

d. São passiveis de ser autorizadas a armazenar, processar e transmitir IC até ao grau de RESERVADO, sistemas com acesso á internet, após conclusão de processo de acreditação e autorização por parte da ANS.

e. São passiveis de ser autorizadas a armazenar, processar e transmitir IC de grau superior a RESERVADO, sistemas sem acesso á internet, após conclusão de processo de acreditação e autorização por parte da ANS.

10. NÍVEL DE SEGURANÇA DAS INTERLIGAÇÕES

a. Definem-se três níveis distintos de segurança que uma interligação pode requerer, designadamente o nível básico, o nível médio e o nível reforçado.

b. **Nível Básico** – interligação que fornece filtragem de pacotes; deteção/prevenção de intrusões; proteção contra *malware*; acesso autorizado e autenticado a funcionalidades de segurança por administradores de segurança; e monitorização do comportamento anormal de funcionalidades de segurança. Constituem-se como cenários deste tipo de interligação:

1) O cenário A - diz respeito a uma interligação com um SIC nacional do mesmo nível de classificação, com a mesma base de segurança e o mesmo contexto operacional, diferindo apenas o CISOA.

c. **Nível Médio** – interligação baseada no nível básico de segurança em que acresce a existência de: separação garantida entre o SIC interno e o SIC externo, com controlos dos fluxos de informação; controlo da difusão e verificação de etiquetas de mensagens; verificação do conteúdo e proteção contra exfiltração de dados. Constituem-se como cenários deste tipo de interligação:

1) O cenário B - diz respeito à interligação com um outro SIC nacional com uma base de segurança diferente ou com um contexto operacional diferenciado e para qualquer grau;
2) O cenário C - diz respeito à interligação de um SIC nacional com um SIC de um país aliado, parceiro, organizações internacionais (IO) ou organizações não governamentais (ONG), para o grau de RESERVADO e inferior;
3) O cenário D - diz respeito à interligação de um SIC nacional de grau RESERVADO com a Internet, ou com um outro SIC nacional NÃO CLASSIFICADO.

d. **Nível Reforçado** – baseia-se no nível de segurança de interligação médio, prevendo um grau de separação mais efetivo entre o SIC interno e o SIC externo; separação entre os fluxos de dados de entrada e de saída; utilização de quebras de protocolo e controlos de fluxo unidirecionais (data *diodes*). Obriga a verificar a conformidade com as políticas de segurança e verifica o formato, a sintaxe e a semântica dos dados. Pode ainda utilizar a transformação de dados para reduzir a complexidade dos dados e permitir a verificação. Proporciona uma separação com elevada confiança na gestão das diferentes funções de segurança. Constituem-se como cenários deste tipo de interligação:

1) O cenário E – diz respeito à interligação de um SIC nacional com um SIC de um país aliado, parceiro, organizações internacionais (IO) ou organizações não governamentais (ONG), para o grau CONFIDENCIAL ou superior.

2) O cenário F – diz respeito à interligação de um SIC nacional com um outro SIC com grau diferente de classificação de segurança, designadamente do grau SECRETO com o grau RESERVADO;
3) O cenário G – diz respeito à interligação de um SIC nacional que trata informação CONFIDENCIAL ou SECRETO com a internet ou redes semelhantes do domínio público, através de um cenário em que apenas permite um fluxo unidirecional que abrange a necessidade de transferir informação específica da Internet para o SIC.

e. A seleção do nível de segurança a aplicar a cada interligação deve ser feita de acordo com a figura 3 em baixo.

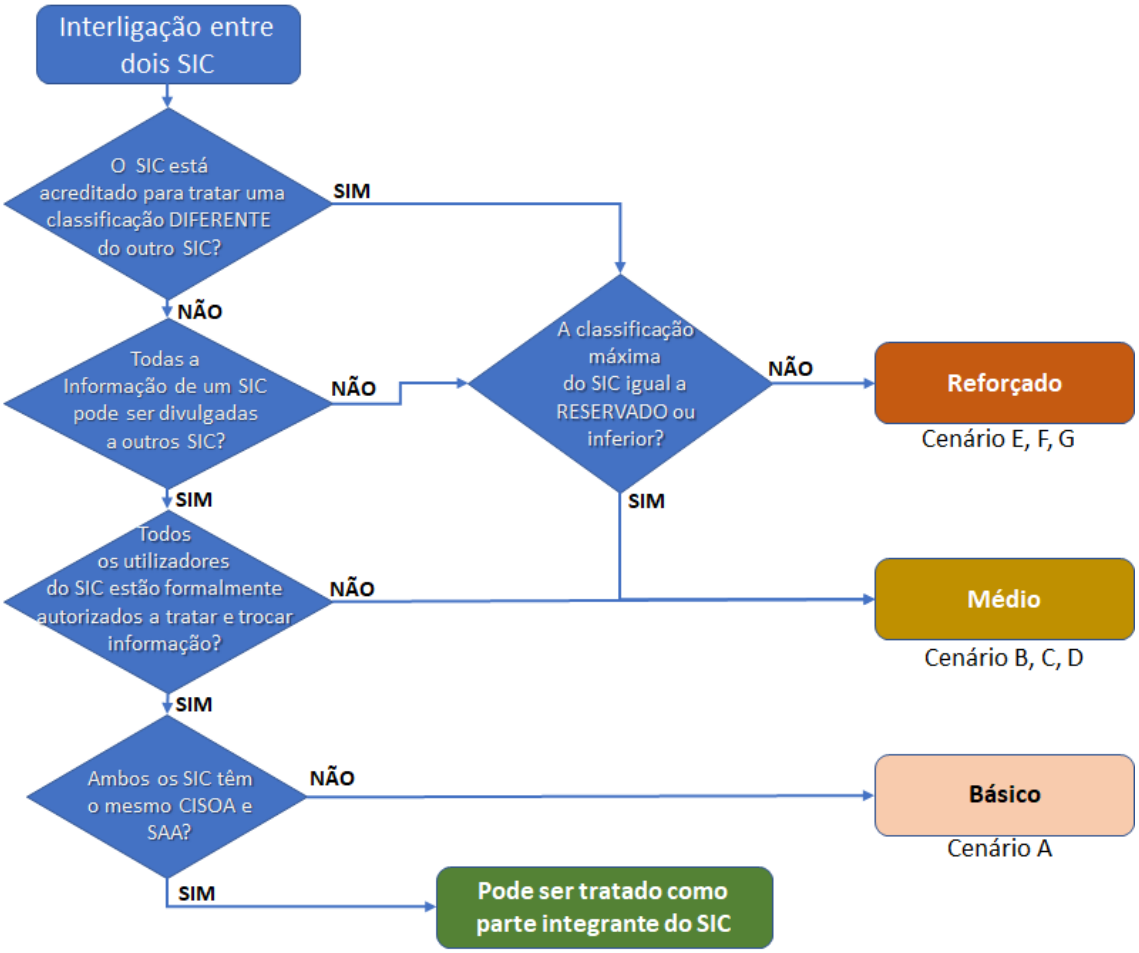

Fig.3 – Fluxograma de identificação do nível de segurança que uma interligação requer.

11. REQUISITOS MINIMIMOS DE SEGURANÇA PARA O PROCESSAMENTO E DISSEMINAÇÃO DE IC

a. Os requisitos mínimos de segurança visam implementar os objetivos e princípios de segurança anteriormente apresentados de forma sistemática, continua e segura, dividindo-se em sete classes e criando uma matriz de requisitos de segurança que se descreve de seguida.

b. A classe **CONFORMIDADE E RESPONSABILIDADE ORGANIZACIONAL** diz respeito ao conjunto de requisitos base de segurança de âmbito básico e regulamentar que visam assegurar o cumprimento e a implementação de processos e procedimentos gerais para utilização de SIC, dividindo-se em:

1) CR1 – Requisitos organizacionais – diz respeito às condições organizacionais mínimas para implementar e operar um SIC no âmbito da IC;
2) CR2 – Maturidade e Capacidade - diz respeito a capacidade e maturidade da organização e que devem ser assegurados de forma cabal por forma e minimizar o risco no âmbito do processamento de IC;
3) CR3 – Políticas e procedimentos existentes para controlo da informação – diz respeito às políticas e procedimentos fundamentais para uma utilização segura de serviços e produtos no âmbito do manuseamento de IC;
4) CR4 – planeamento, desenho e implementação - diz respeito aos requisitos de segurança mínimos para assegurar o planeamento, desenho e implementação correta de um SIC no âmbito da IC;
5) CR5 – treino e sensibilização - diz respeito aos requisitos de segurança mínimos para assegurar o treino e a sensibilização de utilizadores e administradores de um SIC que processa IC;
6) ACR6 – Processo de gestão da configuração - diz respeito aos requisitos de segurança mínimos para assegurar a correta gestão da configuração de um SIC no âmbito da IC;
7) CR7 – Processo de avaliação, certificação e acreditação de tecnologias - diz respeito aos processos formais implementados pela organização para uma utilização segura de serviços e produtos no âmbito do manuseamento de IC.

c. A classe **CONTROLO DE ACESSOS AO SISTEMA** engloba um conjunto de requisitos de segurança de ordem organizacional que visam proteger o acesso ao SIC de forma abrangente, incluindo outros domínios da segurança, como sejam a segurança física, a segurança pessoal, a segurança documental e a segurança da cadeia de abastecimento, dividindo-se em:

1) CO1 – SEGURANÇA FÍSICA – diz respeito aos requisitos de segurança mínimos para assegurar a segurança física de um SIC, no âmbito da IC;

2) CO2 – SISTEMAS DE CONTROLO AMBIENTAL - diz respeito aos requisitos de segurança mínimos para assegurar o controlo do ambiente de operação de um SIC, no âmbito da IC;
3) CO3 – SEGURANÇA DO PESSOAL – diz respeito aos requisitos de segurança mínimos para assegurar a segurança pessoal de um SIC, no âmbito da IC;
4) CO4 – SEGURANÇA INDUSTRIAL (CADEIA DE ABASTECIMENTO) - diz respeito aos requisitos de segurança mínimos para assegurar a segurança industrial e a cadeia de abastecimento que serve um SIC, no âmbito da IC.

d. A classe **SEGURANÇA ELETRÓNICA E DAS COMUNICAÇÕES** diz respeito a requisitos de segurança caracter infraestrutural que visam assegurar a correta implementação de SIC durante a fase de planeamento e edificação, dividindo-se em:

1) SEC1 - ENERGIA - diz respeito aos requisitos de segurança necessários para alimentar eletricamente um SIC no âmbito da IC;
2) SEC2 - CABLAGEM E BASTIDORES – diz respeito aos requisitos de segurança necessários para cadastrar os diferentes módulos de um SIC no âmbito da IC;
3) SEC3 - EXPLORAÇÃO DO ESPECTRO - diz respeito aos requisitos de segurança no âmbito da exploração do espectro eletromagnético de um SIC no âmbito da IC;
4) SEC4 - CONTROLO DE EMISSÃO (*TEMPEST*) - diz respeito aos requisitos de segurança no âmbito do controlo de emissão eletromagnética dos vários módulos de um SIC no âmbito da IC;
5) SEC5 - CONTROLO NA TRANSMISSÃO (*TRANSEC*) - diz respeito aos requisitos de segurança no âmbito da transmissão eletrónica de informação entre os diferentes módulos de um SIC no âmbito da IC.

e. A classe **ARQUITECTURA E DESENHO DO SISTEMA** diz respeito a um conjunto de requisitos mínimos de segurança de ordem estrutural, que visam apoiar a implementação e configuração de um SIC devidamente habilitado a manusear IC, dividindo-se em:

1) ARQ1 – UTILIZAÇÃO DE EQUIPAMENTOS FIXOS (*desktop*) - diz respeito aos requisitos de segurança mínimos para assegurar por qualquer equipamento fixo, tipo *desktop*, que seja utilizado por um SIC no manuseamento de IC;
2) ARQ2 – UTILIZAÇÃO DE DISPOSITIVOS PORTÁTEIS (*laptops*) - diz respeito aos requisitos de segurança mínimos para assegurar por qualquer dispositivo portátil que seja utilizado por um SIC no manuseamento de IC;
3) ARQ3 – UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS (*TABLETS, SMARTPHONES*, ETC…) - diz respeito aos requisitos de segurança mínimos para assegurar por qualquer dispositivo móvel, que seja utilizado por um SIC no manuseamento de IC;

4) ARQ4 – UTILIZAÇÃO DE SUPORTES AMOVIVEIS - diz respeito aos requisitos de segurança mínimos para assegurar a correta utilização de dispositivos amovíveis, tipo *USB PENS*, utilizados por um SIC no manuseamento de IC;
5) ARQ5 – UTILIZAÇÃO DE REDES *ETHERNET* - diz respeito aos requisitos de segurança mínimos necessários para a correta utilização de redes *Ethernet* por um SIC no âmbito da IC;
6) ARQ6 – UTILIZAÇÃO REDES DE TELECOMUNICAÇÕES (UMTS/GSM/LTE/5G) - diz respeito aos requisitos de segurança mínimos necessários para a correta utilização de redes de telecomunicações por um SIC no âmbito da IC;
7) ARQ7 – UTILIZAÇÃO REDES *WIRELESS* (*WI-FI, Bluetooth, DECT*) - diz respeito aos requisitos de segurança mínimos necessários para a correta utilização de redes wireless por um SIC no âmbito da IC;
8) ARQ8 – UTILIZAÇÃO DE PLATAFORMAS EM NUVEM - diz respeito aos requisitos de segurança mínimos necessários para a correta utilização de plataformas em nuvem por um SIC no âmbito da IC;
9) ARQ9 – INTERLIGAÇÕES E INTERNET - diz respeito aos requisitos de segurança mínimos que no âmbito da IC são necessários assegurar para a correta interligação de um SIC, incluindo a ligação á Internet;
10) ARQ10 – CONFIGURAÇÃO *SINGLE-SITE* - diz respeito aos requisitos de segurança mínimos que no âmbito da IC são necessários para a correta configuração de centro de dados de um SIC;
11) ARQ11 – CONFIGURAÇÃO *MULTI-SITE* - diz respeito aos requisitos de segurança mínimos que no âmbito da IC são necessários para a correta configuração de um SIC com vários *sites*.

f. A classe **SEGURANÇA DO SISTEMA DE INFORMAÇÃO** integra um conjunto de requisitos de segurança que visam robustecer um SIC, por forma a proteger a IC produzida, processada e disseminada pelo mesmo, dividindo-se em:

1) SI1 - PROTEÇÃO DO *HARDWARE* E SUPORTES AMOVÍVEIS – diz respeito aos requisitos de segurança adicionais necessários para proteger o *hardware* e os suportes amovíveis de um SIC no âmbito da IC;
2) SI2 - PROTEÇÃO DO *SOFTWARE* - diz respeito aos requisitos de segurança adicionais necessários para proteger o *software* e o *firmware* de um SIC no âmbito da IC;
3) SI3 - PROTEÇÃO DOS SERVIÇOS – diz respeito aos requisitos de segurança adicionais necessários para proteger os serviços de um SIC no âmbito da IC;

4) SI4 - PROTEÇÃO DOS DADOS - diz respeito aos requisitos de segurança adicionais necessários para proteger os dados de um SIC no âmbito da IC;
5) SI4 - PROTEÇÃO DA INFORMAÇÃO - diz respeito aos requisitos de segurança adicionais necessários para proteger a informação de um SIC no âmbito da IC;
6) SI4 - IDENTIDADE E GESTÃO DE ACESSOS - diz respeito aos requisitos de segurança adicionais necessários para proteger a identidade e gerir os acessos a um SIC no âmbito da IC.

g. A classe **MONITORIZAÇÃO CONTINUA E MANUTENÇÃO** diz respeito a requisitos de segurança que visam assegurar uma proteção continua da IC manuseada por um SIC devidamente autorizado ao longo do seu ciclo de vida, dividindo-se em:

1) MCMS1 - DISPONIBILIDADE – diz respeito aos requisitos de segurança para manter a disponibilidade de um SIC no âmbito da IC;
2) MCMS2 - MANUTENÇÃO DA POSTURA DE SEGURANÇA - diz respeito aos requisitos de segurança que devem ser observados pela organização por forma a manter o nível risco residual de processamento de IC dentro dos limites aceitáveis;
3) MCMS3 - MONITORIZAÇÃO CONTINUA, *LOGGING* E AUDITORIA – diz respeito aos requisitos de segurança que devem ser observados pela organização de forma continua no âmbito do manuseamento de IC;
4) MCMS4 - ANALISE DE VULNERABILIDADES - diz respeito aos requisitos de segurança que devem ser implementados pela organização por forma a garantir uma utilização segura de serviços e produtos no âmbito do manuseamento de IC.

h. A classe **GESTÃO DE RISCO E EXPOSIÇÃO** diz respeito a requisitos de segurança que visam assegurar o correto registo, tratamento e acompanhamento de incidentes de segurança, dividindo-se em:

1) GRE1 – GESTÃO DE INCIDENTES – diz respeito às condições organizacionais mínimas para gerir eventos e responder a incidentes de segurança num SIC autorizado a processar IC;
2) GRE2 – GESTÃO DO RISCO – diz respeito às condições organizacionais mínimas gerir o risco de operar um SIC autorizado a processar IC;
3) GRE3 - PLANOS DE CONTINGÊNCIA E DE CONTINUIDADE - diz respeito às condições organizacionais mínimas necessárias para restaurar um SIC ou partes de um SIC no âmbito do processamento de IC.

i. A figura 4 em baixo dá conta da tabela de requisitos mínimos de segurança e no anexo A são detalhados os requisitos mínimos de segurança para cada classe.

LISTA DE REQUISITOS MÍNIMOS DE SEGURANÇA			
CLASSES		REQUISITOS	
CR	CONFORMIDADE COM REGULAMENTAÇÃO	CR1	ORGANIZAÇÃO DE SEGURANÇA PARA CONTROLO DA UTILIZAÇÃO DE TECNOLOGIA
		CR2	MATURIDADE E CAPACIDADE
		CR3	POLITICAS E PROCEDIMENTOS EXISTENTES PARA CONTROLO DA UTILIZAÇÃO DE TECNOLOGIA
		CR4	PROCESSO DE AVALIAÇÃO, CERTIFICAÇÃO E ACREDITAÇÃO DE TECNOLOGIAS
ARQ	ARQUITECTURA E DESENHO DO SISTEMA	ARQ1	PLANEAMENTO, DESENHO E IMPLEMENTAÇÃO
		ARQ2	TREINO E SENSIBILIZAÇÃO
		ARQ3	GESTÃO DA CONFIGURAÇÃO
		ARQ4	UTILIZAÇÃO DE EQUIPAMENTOS FIXOS (HARDWARE)
		ARQ5	UTILIZAÇÃO DE SUPORTES AMOVÍVEIS (USBs; External SDD/HDD; CDs/DVDs, etc)
		ARQ6	UTILIZAÇÃO DE DISPOSITIVOS PORTÁTEIS
		ARQ7	UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS (TABLETS, SMARTPHONES, ETC...)
		ARQ8	UTILIZAÇÃO DE REDES ETHERNET
		ARQ9	UTILIZAÇÃO DE REDES TELECOMUNICAÇÕES (UMTS/GSM/LTE/5G)
		ARQ10	UTILIZAÇÃO DE REDES WIRELESS (WI-FI, Bluetooth, DECT)
		ARQ11	UTILIZAÇÃO DE PLATAFORMAS EM NUVEM
		ARQ12	CONFIGURAÇÃO SINGLE-SITE (CENTRO DE DADOS)
		ARQ13	CONFIGURAÇÃO MULTI-SITE (PRONTO DE PRESENÇA)
		ARQ14	INTERLIGAÇÃO DE SIC E UTILIZAÇÃO DE INTERNET
CO	CONTROLO DE ACESSOS AO SISTEMA	CO1	SEGURANÇA FISICA
		CO2	SISTEMAS DE CONTROLO AMBIENTAL
		CO3	SEGURANÇA DO PESSOAL
		CO4	SEGURANÇA INDUSTRIAL (CADEIA DE ABASTECIMENTO)
SEC	SEGURANÇA ELETRÓNICA E DAS COMUNICAÇÕES	SEC1	ENERGIA
		SEC2	CABLAGEM E BASTIDORES
		SEC3	EXPLORAÇÃO DO ESPECTRO
		SEC4	CONTROLO DE EMISSÃO (TEMPEST)
		SEC5	CONTROLO NA TRANSMISSÃO (TRANSEC)
SSI	SEGURANÇA DO SISTEMA DE INFORMAÇÃO	SSI1	PROTEÇÃO DO HARDWARE E MÍDIA
		SSI2	PROTEÇÃO DO SOFTWARE
		SSI3	PROTEÇÃO DOS SERVIÇOS
		SSI4	PROTEÇÃO DOS DADOS
		SSI5	PROTEÇÃO DA INFORMAÇÃO
		SSI6	IDENTIDADE E GESTÃO DE ACESSOS
MCMS	MONITORIZAÇÃO CONTINUA E MANUTENÇÃO DO SISTEMA	MCMS1	DISPONIBILIDADE
		MCMS2	MANUTENÇÃO DA POSTURA DE SEGURANÇA
		MCMS3	MONITORIZAÇÃO CONTINUA, LOGGING E AUDITORIA
		MCMS4	ANALISE DE VULNERABILIDADES
GRE	GESTÃO DO RISCO E EXPOSIÇÃO	GRE1	GESTÃO DE INCIDENTES
		GRE2	GESTÃO DO RISCO
		GRE3	PLANOS DE CONTINGÊNCIA E DE CONTINUIDADE

Fig.4 – Tabela de requisitos mínimos de segurança para SIC habilitados a manusear IC

12. SELEÇÃO DE REQUISITOS MINIMOS DE SEGURANÇA APLICAVEIS

a. Os requisitos mínimos de segurança encontram-se definidos para o grau de RESERVADO e CONFIDENCIAL e superior.

b. Por forma a permitir a utilização de diferentes arquiteturas, em diferentes contextos, os requisitos mínimos de segurança definidos por esta norma técnica têm por base um princípio cumulativo em função da arquitetura tecnológica que serve de apoio para o processamento de informação classificada, sendo necessário identificar:

1) Aspetos gerais respeitantes a qualquer tipologia de SIC em uso:
   a) Toda a classe de conformidade com a regulamentação;
   b) Toda a classe de controlo de acessos ao sistema;
   c) Toda a classe de segurança eletrónica e das comunicações.
2) Aspetos de arquitetura respeitantes às diferentes tecnologias usadas no processamento de informação classificada ou em apoio desta necessidade, sendo abordadas diferentes perspetivas, designadamente:
   a) No que diz respeito à tipologia:
      (1) Redes Ethernet;
      (2) Redes de Telecomunicações;

(3) Redes Wireless;

(4) Plataformas de Computação em nuvem.

b) Os diferentes tipos de dispositivos em uso:

(1) Equipamento Fixo tipo desktops;

(2) Dispositivos Portátil tipo Laptops;

(3) Dispositivos Amovíveis de memória tipo USB Pens Disk e CD/DVDs;

(4) Dispositivos Móveis tipo Tablets e Smartphones.

c) A capilaridade em uso:

(1) Configuração Stand Alone;

(2) Configuração Single-Site;

(3) Configuração Multi-Site;

d) O contexto em uso:

(1) Tipologia de hardware, software e serviços em uso;

(2) Tipologia de interligação em uso;

(3) A utilização da Internet.

3) Aspetos de continuidade respeitantes a qualquer tipologia de SIC em uso:

a) Toda a classe de monitorização continua e manutenção do sistema;

b) Toda a classe de gestão do risco e da exposição.

c. A seleção dos requisitos aplicáveis a um dado SIC deve ser feita de acordo com a figura 5 em baixo.

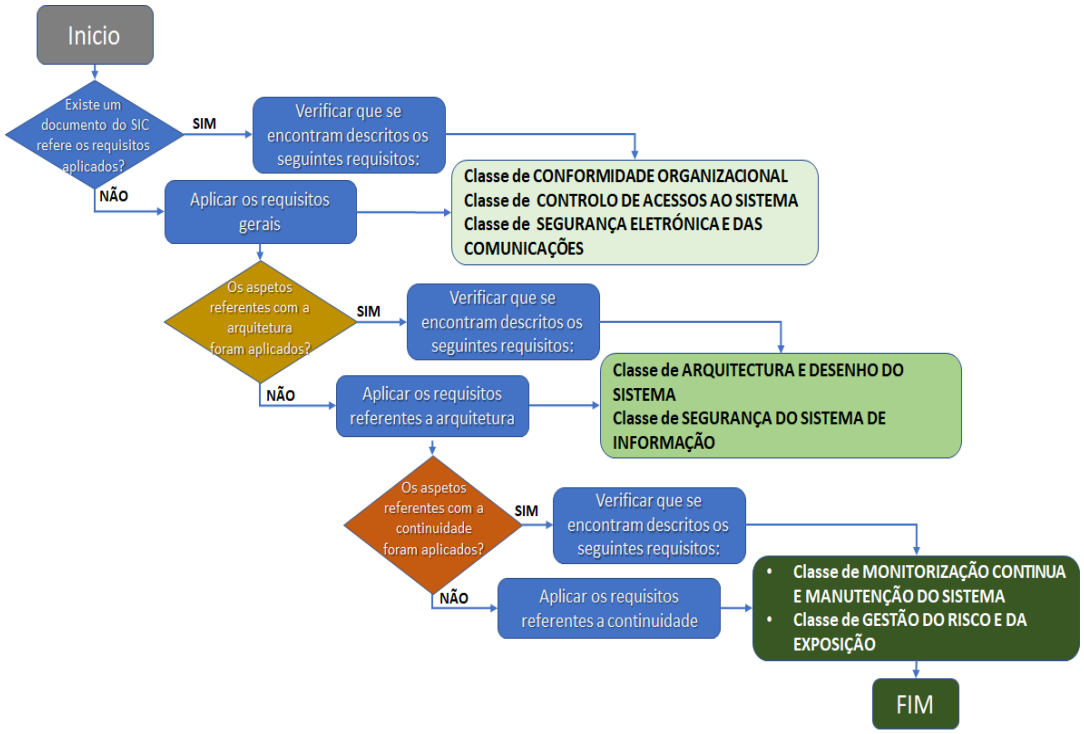

Fig.5 – Fluxograma de apoio para a seleção de requisitos mínimos de segurança a implementar e a auditar no âmbito de um processo de acreditação.

13. CONTROLOS DE SEGURANÇA

a. Para além dos requisitos mínimos de segurança definidos em 11., sempre que se identifiquem desvios deve ser reavaliado o risco e definidos controlos de segurança compensatórios com vista a mitigar ou a reduzir o risco para valores aceitáveis por ambas as partes;

b. Os controlos de segurança visam a implementação de contramedidas ou salvaguardas capazes de evitar, detetar, neutralizar ou minimizar o risco identificado;

c. Para além do descrito nas alíneas anteriores, os controlos de segurança poderão ser identificados aquando da realização de uma avaliação ou auditoria de segurança ao SIC;

d. Compete em qualquer das situações, à ANS aprovar quaisquer controlos de segurança adicionais que venham a ser recomendados para mitigar ou reduzir o risco para valores aceitáveis.

14. ACRÓNIMOS

ANS – Autoridade Nacional de Segurança;

CIS – Ver SIC;

EU – União Europeia;

GNS – Gabinete Nacional de Segurança;

IASP – Information Assurance Security Policy;

IC – Informação Classificada;

IEC – International Electrotechnical Commission;

ISO – International Organization for Standardization;

NT – Norma Técnica;

SecOPs – Security Operating Procedures;

SI – Sistemas de Informação;

SIC – Sistemas de Informação e de Comunicação;

SSRS – System Specific Security Requirement Statement;

TEMPEST – Telecommunications Electronics Material Protected from Emanating Spurious Transmissions;

TIC – Tecnologias de Informação e Comunicação;

TOE – Target of Evaluation;

15. ANEXOS

Anexo A – Requisitos Mínimos de Segurança;

Anexo B – Capacidade e Maturidade organizacional;

16. LISTA DE DISTRIBUIÇÃO

Geral

ANEXO A – REQUISITOS MINIMOS DE SEGURANÇA

[Lista com grau de classificação RESERVADO disponível apenas por solicitação justificada, sujeita à autorização do GNS. O pedido deverá ser feito pelos canais próprios, através do Sub Registo ou Posto de Controlo que apoia a entidade requisitante]

ANEXO B – CAPACIDADE E MATURIDADE

a. O primeiro e principal requisito de segurança para manusear IC ou informação com requisitos especiais de segurança é a criação de uma capacidade mínima para assegurar o processamento e disseminação segura de informação.

b. Neste sentido, existem vários referenciais nacionais e internacionais que definem níveis mínimos de capacidade que as organizações devem possuir, assim como de maturidade organizacional.

c. Sendo o principal referencial nacional o Quadro Nacional de Referência para a Cibersegurança (QNRCS).

d. E a norma ISO/IEC 21827:2008 um destes referenciais internacionais que define as características essenciais para edificar um processo de engenharia de segurança que garanta a proteção dos SIC e da informação por estes tratada.

e. Junto se dá conta, na medida que o referencial nacional é publico, do referencial estabelecido pela norma ISO/IEC 21827:2008 que de forma sumária abrange:

1) todo o ciclo de vida, incluindo atividades de desenvolvimento, operação, manutenção e abate;
2) toda a organização, incluindo atividades administrativas, organizacionais e de engenharia;
3) interações simultâneas com outras disciplinas, como sistemas, software, hardware, fatores humanos e engenharia de teste; gestão, operação e manutenção de sistemas;
4) interações com outras organizações, incluindo aquisição, gestão de sistemas, avaliação, certificação e acreditação.

f. De acordo com a norma ISO/IEC 21827:2008 a determinação da maturidade do processo de engenharia de segurança de uma organização é feita através de duas dimensões, designadas por “domínio” e “capacidade”.

g. A dimensão do domínio consiste em todas as práticas básicas que definem coletivamente a engenharia de segurança, ao passo que a dimensão capacidade representa as práticas genéricas, também designadas por atividades que são atualmente executadas pela organização e que evidenciam a capacidade desta gerir e institucionalizar cada processo.

h. O modelo proposto não inclui requisitos específicos, sendo a organização livre para planear, rastrear, definir, controlar e melhorar os seus processos de qualquer maneira ou sequência que escolher. No entanto, como algumas práticas genéricas de nível superior dependem de

práticas genéricas de nível inferior, as organizações são incentivadas a trabalhar nas práticas genéricas de nível inferior antes de tentar alcançar os níveis mais elevados.

i. Há mais do que uma maneira de agrupar práticas em níveis de capacidade, definindo-se 5 níveis de capacidade, designadamente:

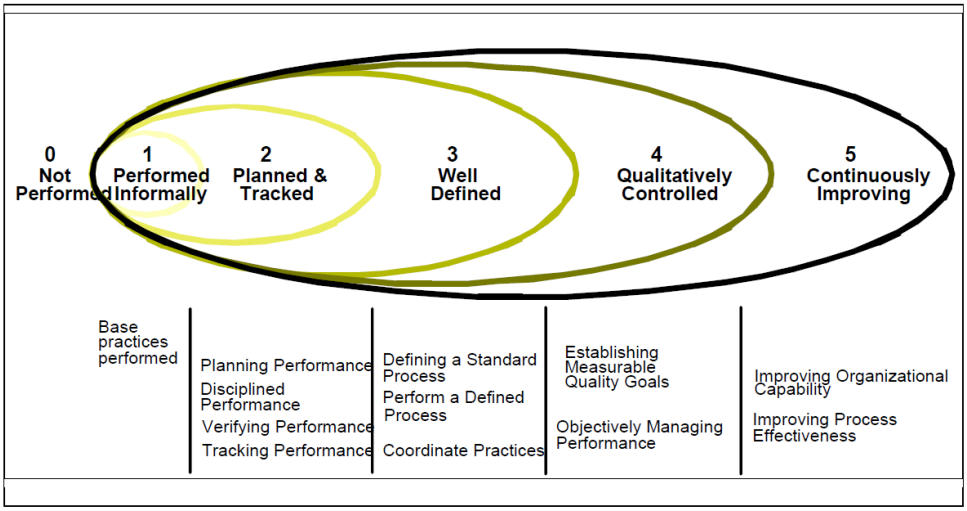

Fig.5 – Níveis de capacidade que representam a maturidade organizacional do processo de engenharia de segurança

j. **Capacidade de Nível 1 - Realizada Informalmente**: As práticas básicas do processo de engenharia de segurança são geralmente executadas. O desempenho dessas práticas básicas pode não ser rigorosamente planeado e acompanhado. O desempenho depende do conhecimento e do esforço individual. Os resultados de cada processo atestam o seu desempenho. Indivíduos dentro da organização reconhecem que uma ação deve ser executada e há um consenso geral de que esta ação é executada como e quando necessário. Existem resultados do trabalho do processo de engenharia de segurança.

k. **Capacidade de Nível 2 - Planeado e Rastreado:** O desempenho das práticas básicas do processo de engenharia de segurança é planeado e acompanhado. Os desempenhos em procedimentos específicos do processo são verificados. Os resultados estão em conformidade com os padrões e com os requisitos de segurança. A aferição é usada para rastrear o desempenho do processo, permitindo que a organização gira as suas atividades com base no desempenho real. A principal distinção para o Nível 1 centra-se no facto do desempenho ser planeado e gerido.

l. **Capacidade de Nível 3 - Bem Definido:** As práticas básicas do processo de engenharia de segurança são executadas de acordo com um processo bem definido usando versões aprovadas e personalizadas de processos padrão devidamente documentados. A principal

distinção para o Nível 2, centra-se no facto do processo ser planeado e gerido usando um processo padrão para toda a organização.

m. **Capacidade de Nível 4 - Controlado Quantitativamente:** Medidas detalhadas de desempenho são recolhidas e analisadas, levando a uma compreensão quantitativa da capacidade do processo e a uma capacidade aprimorada de prever o desempenho. O desempenho é gerido objetivamente e a qualidade dos resultados é quantitativamente conhecida. A principal distinção para o Nível 3, centra-se no facto do processo definido quantitativamente compreendido e controlado.

n. **Capacidade de Nível 5 - Melhoria Contínua:** São estabelecidas metas quantitativas de desempenho para a eficácia e a eficiência dos processos, com base nos objetivos da organização. A melhoria contínua do processo em relação a essas metas encontra-se alicerçado no feedback quantitativo da execução de cada processo e na implementação de ideias e tecnologias inovadoras. A principal distinção para o Nível 4, centra-se no refinamento e na melhoria contínua de cada processo, com base na compreensão quantitativa do impacto das mudanças em cada processo.

ANEXO B1 – MATRIZ DE AVALIAÇÃO DA CAPACIDADE ORGANIZACIONAL EM CONSONÂNCIA COM A NORMA ISO/IEC 21827:2008

CAPABILITY MATURITY LEVEL																																		
Security Engineering Base Pratices			Level 1	Level 2												Level 3								Level 4			Level 5							
			Base Practices are Performed	Planning Performance							Disciplined Performance		Verifying Performance		Tracking Performance	Defining a Standard Process		Perform the Defined Process			Coordinate Practices			Establishing Measurable Quality Goals	Objectively Managing Performance		Improving Organizational Capability	Improving Process Effectiveness						
			Generic Pratices																																
			Perform the Process	Allocate Resources	Assign Responsibilities	Document the Process	Provide Tools	Ensure Training	Plan the Process	Use Plans, Standards, and Procedures	Do Configuration Management	Verify Process Compliance	Audit Work Products	Track with Measurement	Take Corrective Action	Standardize the Process;	Tailor the Standard Process.	Use a Well-Defined Process;	Perform Defect Reviews;	Use Well Defined Data.	Perform Intra-Group Coordination;	Perform Inter-Group Coordination;	Perform External Coordination.	Establish Quality Goals.	Determine Process Capability;	Use Process Capability.	Establish Process Effectiveness Goals;	Continuously Improve the Standard Process.	Perform Causal Analysis;	Eliminate Defect Causes;	Continuously Improve the Defined Process.
Security engineering process areas	PA01 Administer Security Controls	BP.01.01																																
		BP.01.02																																
		BP.01.03																																
		BP.01.04																																
	PA02 Assess Impact	BP.02.01																																
		BP.02.02																																
		BP.02.03																																
		BP.02.04																																
		BP.02.05																																
		BP.02.06																																
	PA03 Assess Security Risk	BP.03.01																																
		BP.03.02																																
		BP.03.03																																
		BP.03.04																																
		BP.03.05																																
		BP.03.06																																
	PA04 Assess Threat	BP.04.01																																
		BP.04.02																																
		BP.04.03																																
		BP.04.04																																
		BP.04.05																																
		BP.04.06																																
	PA05 Assess Vulnerability	BP.05.01																																
		BP.05.02																																
		BP.05.03																																
		BP.05.04																																
		BP.05.05																																
	PA06 Build Assurance Argument	BP.06.01																																
		BP.06.02																																
		BP.06.03																																
		BP.06.04																																
		BP.06.05																																
		BP.06.06																																
	PA07 Coordinate Security	BP.07.01																																
		BP.07.02																																
		BP.07.03																																
		BP.07.04																																
	PA08 Monitor Security Posture	BP.08.01																																
		BP.08.02																																
		BP.08.03																																
		BP.08.04																																
		BP.08.05																																
		BP.08.06																																
		BP.08.07																																
	PA09 Provide Security Input	BP.09.01																																
		BP.09.02																																
		BP.09.03																																
		BP.09.04																																
		BP.09.05																																
		BP.09.06																																
	PA10 Specify Security Needs	BP.10.01																																
		BP.10.02																																
		BP.10.03																																
		BP.10.04																																
		BP.10.05																																
		BP.10.06																																
		BP.10.07																																
	PA11 Verify and Validate Security	BP.11.01																																
		BP.11.02																																
		BP.11.03																																
		BP.11.04																																
		BP.11.05																																

CAPABILITY MATURITY LEVEL

Security Engineering Base Pratices			Level 1	Level 2											Level 3								Level 4			Level 5				
			Base Practices are Performed	Planning Performance							Disciplined Performance		Verifying Performance		Tracking Performance		Defining a Standard Process	Perform the Defined Process			Coordinate Practices			Establishing Measurable Quality Goals	Objectively Managing Performance		Improving Organizational Capability	Improving Process Effectiveness			
			Generic Pratices																												
			Perform the Process	Allocate Resources	Assign Responsibilities	Document the Process	Provide Tools	Ensure Training	Plan the Process	Use Plans, Standards, and Procedures	Do Configuration Management	Verify Process Compliance	Audit Work Products	Track with Measurement	Take Corrective Action	Standardize the Process;	Tailor the Standard Process.	Use a Well-Defined Process;	Perform Defect Reviews;	Use Well Defined Data.	Perform Intra-Group Coordination;	Perform Inter-Group Coordination;	Perform External Coordination.	Establish Quality Goals.	Determine Process Capability;	Use Process Capability.	Establish Process Effectiveness Goals;	Continuously Improve the Standard Process.	Perform Causal Analysis;	Eliminate Defect Causes;	Continuously Improve the Defined Process.
Project and organization process areas	PA12 Ensure Quality	BP.12.01																												
		BP.12.02																												
		BP.12.03																												
		BP.12.04																												
		BP.12.05																												
		BP.12.06																												
		BP.12.07																												
		BP.12.08																												
	PA13 Manage Configuration	BP.13.01																												
		BP.13.02																												
		BP.13.03																												
		BP.13.04																												
		BP.13.05																												
	PA14 Manage Project Risk	BP.14.01																												
		BP.14.02																												
		BP.14.03																												
		BP.14.04																												
		BP.14.05																												
		BP.14.06																												
	PA15 Monitor and Control Technical Effort	BP.15.01																												
		BP.15.02																												
		BP.15.03																												
		BP.15.04																												
		BP.15.05																												
		BP.15.06																												
	PA16 Plan Technical Effort	BP.16.01																												
		BP.16.02																												
		BP.16.03																												
		BP.16.04																												
		BP.16.05																												
		BP.16.06																												
		BP.16.07																												
		BP.16.08																												
		BP.16.09																												
		BP.16.10																												
	PA17 Define Organization's Systems Engineering Process	BP.17.01																												
		BP.17.02																												
		BP.17.03																												
		BP.17.04																												
	PA18 Improve Organization's Systems Engineering Process	BP.18.01																												
		BP.18.02																												
		BP.18.03																												
		BP.18.04																												
	PA19 Manage Product Line Evolution	BP.19.01																												
		BP.19.02																												
		BP.19.03																												
		BP.19.04																												
		BP.19.05																												
	PA20 Manage Systems Engineering Support Environment	BP.20.01																												
		BP.20.02																												
		BP.20.03																												
		BP.20.04																												
		BP.20.05																												
		BP.20.06																												
		BP.20.07																												
	PA21 Provide Ongoing Skills and Knowledge	BP.21.01																												
		BP.21.02																												
		BP.21.03																												
		BP.21.04																												
		BP.21.05																												
		BP.21.06																												
		BP.21.07																												
		BP.21.08																												
	PA22 Coordinate with Suppliers	BP.22.01																												
		BP.22.02																												
		BP.22.03																												
		BP.22.04																												
		BP.22.05																												