Gabinete Nacional de Segurança
PORTUGAL

Esquema de Avaliação e Certificação em Segurança Tecnológica de produtos habilitados para processamento de Informação Classificada

Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Página de Controlo

Bloco de autorização

ENDOSSADO POR: José Gonçalves Coronel	NOME: José Carlos Gonçalves Digitally signed by José Carlos Gonçalves Date: 2025.04.28 18:35:50 +01'00'
ASSINATURA:	DATA:
REVISTO POR: Carla Santos Coronel	NOME:
ASSINATURA:	DATA:
AUTORIZADO POR: António José Gameiro Marques Contra-Almirante	TITLE: AUTORIDADE NACIONAL DE SEGURANÇA
ASSINATURA:	DATA: António José Gameiro Marques Digitally signed by António José Gameiro Marques Date: 2025.04.29 09:11:25 +01'00'

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Referências

Nacionais:

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

Europeias:

- 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);
- 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;
- 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;
- Information Assurance (IA) Security Policy on Security Throughout the CIS Life Cycle – IASP-L;
- IA Security Policy on Security Governance – IASP-G;
- IA Security Policy on Risk Management – IASP 1;
- IA Security Policy on Interconnection – IASP 3;
- IA Security Policy on Network Defence – IASP 4;
- IA Security Policy on CIS Security Engineering – IASP 5;
- IA Security Policy on Qualification and Approval of non-cryptographic Products – IASP 6;
- IA Security Policy on TEMPEST – IASP 7;
- 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 e que revoga o Regulamento (UE) n. o 526/2013 (Regulamento Cibersegurança);
- EUCC – European Cybersecurity Certification Scheme, version 1.1.1 dated May 25, 2021;

NATO:

- C-M(2002)49 NATO Security Policy;
- AC/35-D/2004 – Primary Directive on CIS Security;
- AC/35-D/2005 – Management Directive on CIS Security;
- AC/35-D/1019 – Guidelines for the Security Evaluation and Certification of CIS;
- AC/35-D/1017 – Guidelines for the Security Risk Management of CIS;
- AC/35-D/1039 – Guidelines on Business Continuity Planning for CIS;
- AC/35-D/2001 – Directive on Physical Security;
- C/322-D(2004)0021 – Directive for the Electronic labelling of NATO information;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- AC/322-D(2005)0043 - Directive for the Assessment of Assurance Levels in Specific CIS Environments;
- AC/322-D(2006)0006 - Directive on the use of the Common Criteria Within NATO;
- AC/322-D(2007)0043 – Supporting Document on the Availability aspects of security;
- AC/322-D(2010) 0042 – INFOSEC Technical and Implementation Directive for the NATO Information Assurance Product Catalogue (NIAPC);
- AC/322-D(2019)0041 (INV) - Technical and Implementation Directive on Introducing Secure Systems and Solutions Using Commercial Off the Shelf (COTS) Products into NATO;
- AC/322-D/0048 - Directive on Computer & Local Area Network (LAN) Security;
- AC/322-D/0049 - Directive for Transmission Security;
- AC/322-D/0050 - Directive on Emission Security;
- AC/322-D/0030 - Directive for the Interconnection of CIS;
- SDIP 27 – NATO TEMPEST Requirements and Evaluation Procedures.

Internacionais:

- [ISO Guide 73] ISO Guide 73:2009, Risk management — Vocabulary;
- [ISO9000] ISO 9000:2015, Quality management systems — Fundamentals and Vocabulary;
- [ISO15408-3] ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components;
- [ISO18045] ISO/IEC 18045:2022, Information technology – Security techniques – Methodology for IT security evaluation;
- [ISO17000] ISO/IEC 17000:2020, Conformity assessment – Vocabulary and general principles;
- [ISO17020] ISO/IEC 17020:2012 - Conformity assessment — Requirements for the operation of various types of bodies performing inspection;
- NP EN ISO/IEC 17020:2013 Avaliação da conformidade – Requisitos para o funcionamento de diferentes tipos de organismos de inspeção;
- [ISO17021] ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management ;
- [ISO17025] ISO/IEC 17025:2017, General requirements for the competence of testing and calibration laboratories;
- [ISO17029] ISO/IEC 17029:2019, Conformity assessment — General principles and requirements for validation and verification bodies;
- [ISO17065] ISO/IEC 17065:2012, Conformity assessment — Requirements for bodies certifying products, processes and services;
- [ISO17067] ISO/IEC 17067:2013, Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes;
- [ISO17788] ISO/IEC 17788:2014, Information technology – Cloud computing – Overview and Vocabulary;
- [ISO19011] ISO 19011:2018, Guidelines for auditing management systems;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- [ISO20000-10] ISO/IEC 20000-10:2019, Information technology – Service management – Part 10: Concepts and Vocabulary;
- [ISO24765] ISO/IEC/IEEE 24765:2017, Systems and software engineering — Vocabulary;
- [ISO27000] ISO/IEC 27000:2018, Information technology – Security techniques – Information security management systems – Overview and Vocabulary;
- [ISO27001] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements;
- [ISO27005] ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management;
- [ISO27006] ISO/IEC 27006:2015, Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems;
- [ISO27007] ISO/IEC 27007:2020, Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing;
- [ISO27017] ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services;
- [ISO29147] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure;
- [ISO30111] ISO/IEC 30111:2019, Information technology — Security techniques — Vulnerability handling processes.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Índice

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

1. Introdução e síntese

A crescente utilização de **Tecnologias de Informação e Comunicação** (TIC) no processamento de **Informação Classificada (IC)** desencadeou a necessidade de certificar produtos, serviços e processos tecnológicos, designados adiante em conjunto somente por produtos, que minimizem o risco inerente à sua utilização.

Neste sentido, é essencial edificar um esquema de certificação nacional, no âmbito da segurança tecnológica da IC, que garanta a segurança, a confiança e a transparência por meio da respetiva conformidade de produtos usados para o processamento desse tipo de informação.

O presente **Esquema de Avaliação e Certificação em Segurança Tecnológica de Produtos Habilitados para Processamento de Informação Classificada,** adiante apenas referido por **Esquema**, representa um investimento na segurança da IC, prevenindo perdas ou comprometimento de informação e respetivos custos associados, revelando-se também um fator de distinção dos produtos pela inovação no âmbito da segurança tecnológica, na fase de produção ou de integração de tecnologia, promovendo potenciais retornos para todas as organizações.

1.1. Atribuições e competências

Nos termos do Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual, a Autoridade Nacional de Segurança (ANS) dirige o Gabinete Nacional de Segurança (GNS) e é a entidade que exerce, em exclusivo, a proteção, o controlo e a salvaguarda da IC em Portugal.

Ainda de acordo com o mesmo diploma legal, o GNS tem por atribuição avaliar e certificar os produtos que tenham como finalidade o processamento, arquivo e transmissão de IC em território nacional, sendo a certificação conferida pela ANS.

1.2. Objetivo

A certificação em Segurança Tecnológica tem por objetivo avaliar e certificar o grau de segurança e de confiança de um produto para o processamento de IC, em conformidade com os requisitos de segurança da informação e os procedimentos constantes do presente Esquema.

O presente Esquema destina-se às entidades do setor público e privado, que desenvolvam atividade no território nacional, e que pretendam ver os seus produtos certificados para processamento de IC.

Para a obtenção da certificação de segurança de um produto, é necessária a avaliação de segurança prévia do produto.

As avaliações de segurança dos produtos são realizadas por Organismos de Avaliação da conformidade (OAV) autorizados pelo GNS, na qualidade de Organismo de Certificação da Conformidade (OCC).

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

O modelo preconizado pelo presente Esquema assenta na existência de um único Organismo de Certificação da Conformidade (OCC), o Gabinete Nacional de Segurança (GNS), e em múltiplos Organismos de Avaliação da conformidade (OAV), autorizados pelo OCC para essa atividade.

1.5. Alterações

O GNS reserva-se o direito de alterar o presente Esquema, nomeadamente quando ocorram alterações dos requisitos definidos nos documentos de referência do presente Esquema.

As alterações ao Esquema serão publicadas no portal do GNS, ficando em destaque na página principal durante 60 dias. Caso as alterações ao Esquema impliquem alterações nos produtos que se encontrem já certificados, as respetivas entidades serão contactadas para efeitos de atualização do produto.

1.6. Definições

Avaliação de Segurança – Aferição imparcial feita sobre um produto, por um órgão independente e autorizado para o efeito, 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 sujeito a avaliação dá-se o nome de *Target of Evaluation* (TOE).

Certificação de Segurança – Procedimento pelo qual uma entidade certificadora atesta que um produto, tendo presente uma avaliação de segurança para o efeito, depois de avaliado, está em conformidade com os requisitos de segurança pré-definidos para uma dada marca e grau.

Ciclo de certificação - Período que se inicia com a atribuição da certificação até ao final da validade do certificado, e durante o qual o GNS, na qualidade de OCC, realiza um conjunto de atividades de avaliação para verificação do cumprimento dos requisitos da certificação pela entidade certificada.

Certificado de conformidade – Declaração emitida pelo GNS, na qualidade de OCC, que atesta a conformidade de um produto para com um Perfil de Proteção (PP).

"Security by Design"[1] **–** Abordagem à segurança tecnológica de um produto TIC, desde a sua conceção, procurando integrar em todo o processo de engenharia, desde o seu desenho, desenvolvimento e nas fases de testes, padrões de segurança de forma holística, criativa, proativa, interdisciplinar, robusta, responsável e integrada.

"Security by Default"[2] – Abordagem à configuração de produtos, no sentido de garantir uma configuração segura desde a versão base do produto, ou a utilização padrão (*by default*) do

[1] 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;

[2] Tradução livre de REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), disponível em:

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

mesmo, ainda que não seja a mais fácil de utilizar, sendo definida por normas ou referenciais extraídos de uma análise do risco e/ou de testes de verificação.

Entidade Requerente (EReq) – Entidade pública ou privada, nomeadamente operador económico ou outra pessoa jurídica, inclusive singular, representada por quem tem poderes para a obrigar, que requer a avaliação e certificação de um produto em conformidade com o presente Esquema.

Esquema de certificação - Conjunto de requisitos e procedimentos para a realização da certificação de produtos.

Mecanismo de segurança – Ferramentas e técnicas usadas para implementar um requisito de segurança de forma confiável e segura. Um mecanismo de segurança pode operar sozinho ou em conjunto com outros para assegurar a correta implementação de um requisito de segurança.

Não Conformidade (NC) – Falta de cumprimento de um requisito previsto no presente Esquema.

Nível de Proteção (NP) – Indicador que visa assegurar a implementação do conceito "*Security by Default*", através da relação entre mecanismos de segurança existentes no produto versus os mecanismos de segurança configurados por defeito. É calculado de acordo com a seguinte fórmula:

$$NP = 1 - \frac{(MSt - MSd)}{(MSt + MSd)}$$

NP - Nível de proteção;
MSt – Nº total de mecanismos de segurança existentes no produto;
MSd – Nº de mecanismos de segurança configurados por defeito no produto;

Nível de Garantia de Segurança – Indicador composto que agrega todos os requisitos exigidos pelo presente Esquema, permitindo caracterizar os seguintes três níveis de garantia de segurança distintos: **"BÁSICO", "MELHORADO" e "SUPERIOR"**.

Objeto de avaliação – Produto sujeito a avaliação, também designado por *Target of Evaluation* (TOE), que inclui todos os componentes que não estando sujeitos a quaisquer reivindicações de segurança, podem interferir na capacidade do hardware, software e firmware satisfazer os seus requisitos funcionais, bem como, toda a documentação de operação, configuração e utilização.

Operador económico[3] – Designa o fabricante, importador ou distribuidor do produto;

Organismo de Avaliação da conformidade (OAV) – Entidade responsável pela condução de avaliações de segurança dos produtos para efeitos da sua certificação em conformidade com o presente Esquema.

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN , consultada em 17/08/2020;

[3] Conforme definido pela DECISÃO Nº 768/2008/CE DO PARLAMENTO EUROPEU E DO CONSELHO de 9 julho de 2008 relativa a um quadro comum para a comercialização de produtos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Organismo de certificação da conformidade (OCC) – GNS, na qualidade de entidade responsável pela certificação de segurança de produtos.

Perfil de Proteção (PP) – Conjunto independente de requisitos de implementação e objetivos de segurança para uma categoria de produtos, que atendem a necessidades de segurança semelhantes. A elaboração de um PP tem por base um processo de gestão do risco a partir do qual se devem definir os requisitos de funcionalidade e de garantia de segurança de forma eficaz e útil para o cumprimento dos objetivos de segurança identificados.

Produto - Resultado de um processo de desenvolvimento que se traduz em *software*, *hardware* ou a combinação de ambos (equipamento). O termo produto neste Esquema também pode designar processo ou serviço indistintamente ou em conjunto, exceto quando os termos forem empregues autonomamente nos respetivos âmbitos.

Requisito – Requisito relativo a um produto, especificado em normas ou em outros documentos de referência identificados pelo presente Esquema e que tem de ser satisfeito pela EReq como uma condição para a obtenção ou renovação da certificação do produto.

Serviço – Prestação de atividade de intermediação executada através de uma infraestrutura, plataforma ou *software* detidos por prestadores de serviços e disponibilizado a múltiplos utilizadores através da Internet, facilitando o fluxo de dados entre diferentes serviços e entidades.

Tecnologias de Informação e de Comunicação (TIC) – Conjunto diversificado de ferramentas e recursos tecnológicos utilizados para transmitir, armazenar, criar, compartilhar ou trocar informação. Essas ferramentas e recursos tecnológicos incluem computadores, a Internet, tecnologias de transmissão, tecnologias de gravação e de telecomunicação (fixa ou móvel, satélite, etc.).[4]

Vulnerabilidade – Deficiência no produto que pode permitir a sua exploração por pessoas não autorizadas ou criar quebras de segurança.[5]

[4] Tradução livre de: http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict , consultada em 17/08/2020;
[5] Tradução livre de: ISO/IEC 27000:2018, disponível em https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27000:ed-5:v1:en , consultada em 26/02/2022

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

1.7. Glossário

ANS – Autoridade Nacional de Segurança

ENISA – Agência da União Europeia para a Cibersegurança

EReq – Entidade Requerente

GNS – Gabinete Nacional de Segurança

IC – Informação Classificada

IPAC – Instituto Português de Acreditação, I.P.

ISO/IEC – Organização internacional de normalização/ Comissão eletrotécnica internacional

NATO – *North Atlantic Treaty Organization*

NC – Não Conformidade

OAV – Organismo de Avaliação da conformidade

OCC – Organismo de Certificação da Conformidade

PAC – Plano de Ações Corretivas

RAT – Relatório de Avaliação Técnica

TIC – Tecnologia de Informação e Comunicação

TOE – *Target of Evaluation*

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

2. Esquema de Certificação

Na Figura 1 apresenta-se o fluxograma do processo de avaliação e certificação, de forma simplificada, com as interações entre a Entidade Requerente (EReq), o Organismo de Avaliação da Conformidade (OAV) e o Organismo de certificação da conformidade (OCC)[6].

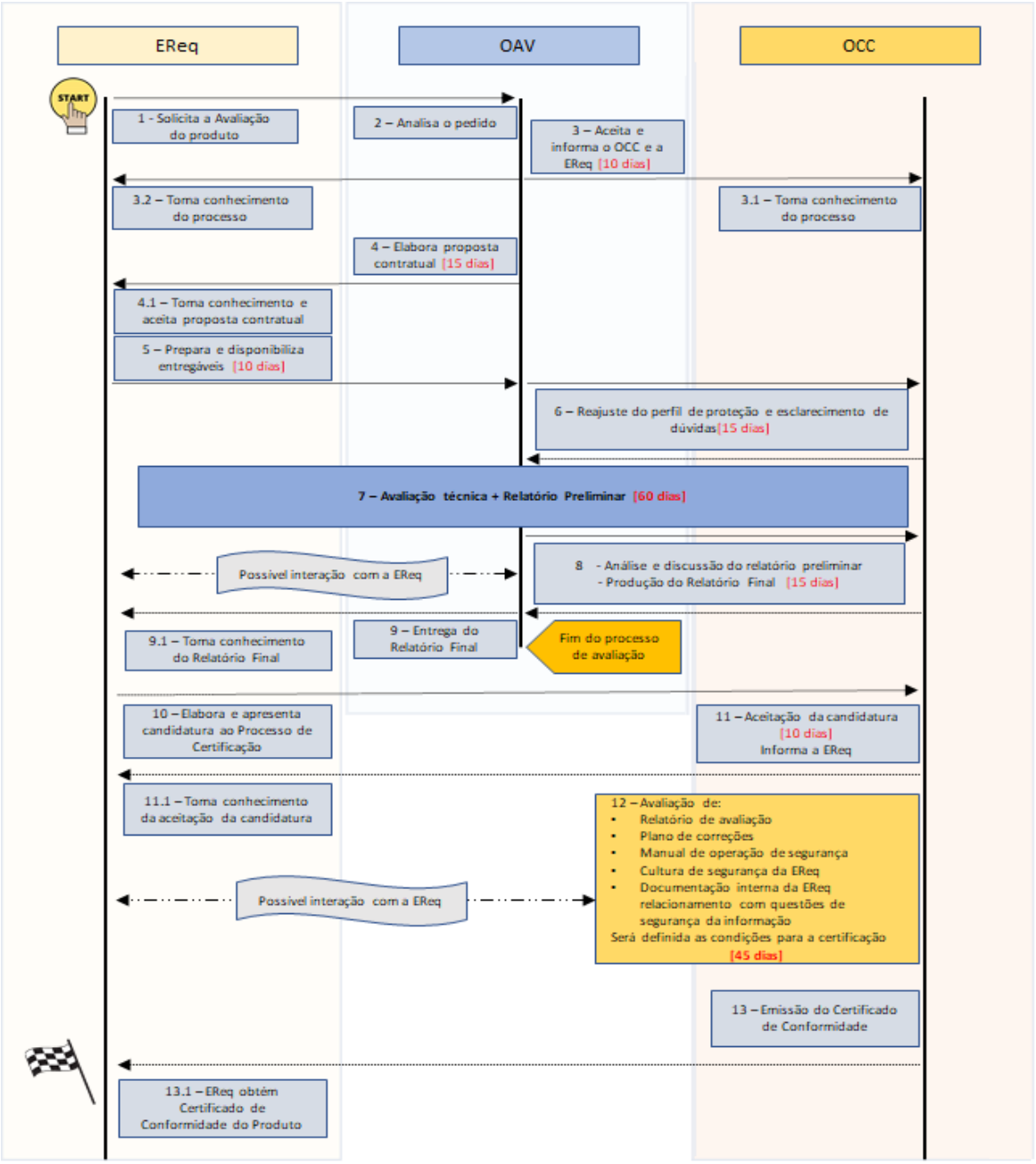

Figura 1 - Fluxograma do processo de avaliação e certificação

Os prazos apresentados são os considerados adequados para a execução de um processo de certificação da conformidade que decorra dentro da normalidade, sendo expetável que o mesmo seja concluído em cerca de 6 meses.

[6] O OCC é o Gabinete Nacional de Segurança

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

2.1. Responsabilidades do Organismo de Certificação da Conformidade (OCC)

O presente Esquema tem como OCC o GNS.

São responsabilidades do GNS:

- Aprovar os perfis de proteção para cada tipo de produto sujeito a certificação.
- Prestar os esclarecimentos necessários sobre o processo de certificação.
- Divulgar os produtos certificados.
- Manter atualizado o presente Esquema de modo a manter a coerência com a evolução dos normativos equiparados a nível nacional e internacional.
- Estabelecer a ligação com as agências nacionais e internacionais apropriadas para o reconhecimento mútuo de certificados.
- Emitir Certificados de Conformidade sobre produtos quando a Entidade Requerente cumprir com sucesso o estipulado no Esquema.

2.2. Responsabilidades do Organismos de Avaliação da Conformidade (OAV)

Podem constituir-se como OAV as entidades estabelecidas em Portugal que pretendam fornecer um serviço de avaliação, desde que devidamente autorizadas pelo GNS.

São responsabilidades do OAV:

- Propor equipa de avaliação mediante o produto a ser avaliado.
- Propor e aplicar os perfis de proteção adequados mediante as especificações do produto, a marca e grau pretendido, em consonância com as orientações do OCC.
- Aplicar o estipulado no presente Esquema.
- Aplicar os padrões de confidencialidade comercial, integridade e imparcialidade, nomeadamente estabelecendo acordos de confidencialidade com as diversas entidades.
- Estar em condições de poder repetir os ensaios ou testes efetuados.
- Ter os seus colaboradores e avaliadores individuais devidamente credenciados pelo GNS.
- Nos casos exigidos pelo presente Esquema, ser acreditado pelo IPAC.

2.4. Classes, categorias e tipos de produto

Os produtos distribuem-se pelas seguintes classes e categorias:

Classe Produtos	Categoria Produto
Produtos Comerciais Não Criptográficos	Produtos de comunicações móveis seguras
	Produtos físicos de computação
	Produtos de rede
	Produtos de autenticação
	Produtos especificos de utilização Governamental
Produtos Criptográficos	Módulos Cripto
	Produtos Criptografia de armazenamento
	Produtos Criptografia de Transmissão
	Produtos de Gestão de Chaves
Produtos Baixa Radiação (TEMPEST)	Tipo A
	Tipo B
	Tipo C
Serviços de Computação em Nuvem	*Infrastruture as a Service (IAAS)*
	Platform as a Service (PAAS)
	Software as a Service (SAAS)
	Third Party Applications

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Existem 42 tipos de produtos cuja lista pode ser consultada no Formulário de Candidatura de Organismos de Avaliação da Conformidade (Anexo I, parte 5).

2.5. Tipos de certificação

Sem prejuízo do GNS poder integrar outros tipos de certificação que obedeçam a regras e atividades diferentes, o presente Esquema compreende os seguintes tipos de certificação:

- **"ISOLADO"**, é um esquema tipo 3 segundo a NP EN ISO/IEC 17067:2013, sendo o produto certificado em resultado de uma avaliação inicial a uma ou mais amostras do produto, e regularmente submetido a atividades de acompanhamento que envolvem a retirada periódica de amostras do produto do mercado e sua submissão a atividades de avaliação para verificação do cumprimento dos requisitos;
- **"LOTE"**, é um esquema tipo 1b segundo a NP EN ISO/IEC 17067:2013, que compreende a avaliação de um lote completo do produto segundo as atividades definidas no presente Esquema;
- **"COMPLETO"**, é um esquema tipo 5 segundo a NP EN ISO/IEC 17067:2013, que compreende a avaliação do produto, do processo de produção, do sistema de gestão, e do impacto da cadeia de abastecimento no produto. As atividades de acompanhamento aplicáveis ao produto certificado permitem escolher entre retirar periodicamente amostras do produto do ponto de produção, retirar amostras do mercado, ou de ambos, e submetê-las às atividades de avaliação para verificação do cumprimento dos requisitos especificados. O acompanhamento inclui, ainda, a avaliação periódica do processo de produção, auditoria ao sistema de gestão, ou ambos;
- **"SERVIÇO"**, é um esquema tipo 6 segundo a NP EN ISO/IEC 17067:2013, e destina-se à avaliação de serviços. As atividades de avaliação de um serviço incluem a avaliação dos elementos intangíveis, como a eficácia de procedimentos, e a avaliação dos elementos tangíveis, como a eficácia de controlos e as atividades de inspeção e auditoria realizadas. As atividades de avaliação de um serviço podem incluir testes e inspeções a amostras resultantes desse processo, sendo as atividades de acompanhamento realizadas de forma periódica ao serviço.

Apresenta-se abaixo a relação dos tipos de certificação e as classes de produto, bem como o enquadramento normativo e respetivas referências:

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Classes de produtos:	Productos Comerciais Não Criptográficos	Computação em nuvem	Criptografia	Baixa Radiação (TEMPEST)
1. Objeto	Produtos	Serviços	Produtos	Produtos
2. Âmbito	NACIONAL	NACIONAL	NACIONAL, NATO & UE	NACIONAL, NATO & UE
3. Enquadramento normativo	EN ISO/IEC 17020 EN ISO/IEC 17025	EN ISO/IEC 17020	EN ISO/IEC 17020 EN ISO/IEC 17025	EN ISO/IEC 17025
4. Tipo de Certificação	ISOLADO; LOTE	SERVIÇO	COMPLETO	ISOLADO
5. Base	• *Commom Criteria.*	• *Cloud Security Alliance*	• NATO & UE	• NATO & UE
6. Referências	• ISO/IEC 15408; • ISO/IEC 18045; • NIST SP800-53 R5;	• CSA Matrix (CCM) V4.0.1 ; • NATO: AC/35-D/1050; • ENISA Cybersecurity Certification of Cloud Services;	• NATO Directive on Cryptographic Security and Cryptographic Mechanisms; • IA Security Policy on Cryptography – IASP 2;	• NATO Directive on Emission Security; • SDIP 27/2 – TEMPEST; • IA Security Policy on TEMPEST – IASP 7;

2.5. Requisitos gerais do produto para ser certificado

Constituem-se como requisitos gerais de admissão do produto para certificação:

Requisito 1: as versões do produto devem ser identificadas de forma exclusiva, podendo ser completamente recriadas posteriormente, com a rastreabilidade fornecida pelo (s) identificador (s) usado;

Requisito 2: o produto deve ser caracterizado através dos seus diferentes módulos e componentes, identificando as suas dependências internas e externas;

Requisito 3: o processo de implementação e configuração deve ser consistente e repetível, ou seja, o mais automatizado possível;

Requisito 4: a EReq deve possuir um processo interno de gestão de vulnerabilidades do produto e um mecanismo de comunicação para o utilizador que disponibilize correções ou novas versões, assim como, para receção de reportes de quaisquer problemas ou sugestões pelos utilizadores;

Requisito 5: a EReq deve possuir um mecanismo de auditoria interno que identifique o autor de qualquer alteração à configuração de um módulo ou componente do produto;

Requisito 6: a EReq deve fornecer sobre o modelo de montagem, implementação ou programação utilizado as evidências necessárias de que este assegura que não são propagados defeitos comuns nem introduzidas no produto deficiências de segurança;

Requisito 7: a EReq deve fornecer as evidências necessárias sobre os processos de gestão implementados para garantir a segurança do produto e a atualização do mesmo ao longo do seu ciclo de vida;

Requisito 8: a EReq deve caracterizar o ambiente de segurança para o qual o produto foi desenvolvido, designadamente quais os mecanismos de segurança disponibilizados e implementados por defeito no seu produto;

Requisito 9: a EReq deve permitir que sejam realizadas auditoria por parte do OCC, de forma coordenada;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Requisito 10: a EReq deve estar em condições de partilhar informação com o Gabinete Nacional de Segurança sempre que concluir que existe ou poderá haver um incidente de segurança com impacto relevante para a informação classificada;

Requisito 11: a EReq deve, para desenvolver produtos de nível Melhorado ou Superior, possuir um ambiente em conformidade com o descrito no Anexo G ao presente Esquema;

Requisito 12: a EReq deve identificar a utilização do produto em cenários de manuseamento de informação classificada e reivindicar a conformidade do seu produto para com um nível de garantia.

2.6. Requisitos específicos do produto para ser certificado

Para além dos requisitos gerais, a avaliação e certificação de um produto é suportada por requisitos específicos associados a mecanismos de segurança e requisitos de garantia de segurança que o produto oferece. Para cada uma das classes de produtos, aplicam-se os seguintes requisitos de acordo com os respetivos anexos:

- Produtos Comerciais não Criptográficos – Anexo B e Anexo F
- Produtos Criptográficos – Anexo C e Anexo F
- Produtos de Baixa Radiação (TEMPEST) – Anexo D
- Serviços de Computação em Nuvem – Anexo E

Para os ambientes de desenvolvimento dos produtos de nível Melhorado ou Superior (de qualquer classe), devem ainda ser garantidos os requisitos mínimos de segurança previstos no Anexo G.

2.7. Marcas e etiquetas

A certificação da conformidade de acordo com o presente Esquema confere a um produto o respetivo certificado e o direito ao uso da marca e etiqueta da certificação conferida pelo GNS, atestando que o produto está conformidade com os requisitos de segurança previstos no presente Esquema para processar IC no grau de segurança em que foi certificado, promovendo assim a segurança da informação e a competitividade do produto.

A marca e etiqueta associada à certificação só podem ser utilizadas relativamente ao produto certificado e durante o período da respetiva validade.

O uso indevido do certificado ou o abuso da marca e/ou da etiqueta ou o incumprimento das regras previstas no presente Esquema determinam a abertura de processo pela ANS para apuramento de responsabilidades, que pode determinar a suspensão, anulação ou revogação da certificação que tenha sido conferida, sem prejuízo de outras consequências legais, no âmbito da responsabilidade civil e criminal, nomeadamente por violação de direitos da propriedade intelectual e de direitos do consumidor.

2.8. Segurança da informação

Salvo disposição legal em contrário, todos os intervenientes na aplicação do presente Esquema devem respeitar a confidencialidade da informação disponibilizada e dos dados obtidos no âmbito do processo de avaliação e de certificação, a fim de proteger:

a) Dados pessoais, de acordo com o RGPD e outra regulamentação aplicável neste âmbito;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

b) Segredos comerciais de qualquer pessoa singular ou coletiva, incluindo direitos de propriedade intelectual;

c) Informações necessárias para a implementação eficaz do presente Esquema, incluindo no tratamento das reclamações.

2.9. Condições financeiras

O processo de avaliação e de certificação envolve o pagamento de serviços e de taxas conforme aplicável.

Os serviços de avaliação junto do OAV são contratados pela EReq, suportando o respetivo custo.

O processo de avaliação e certificação pelo GNS é faturado conforme previsto na Portaria n.º 283/2014, de 31 de dezembro, na sua redação atual, disponível no link, sendo da responsabilidade da EReq proceder ao seu pagamento.

De acordo com o nº 1 do artigo 4º da referida Portaria, os serviços prestados pelo GNS a micro, pequenas e médias empresas (PME) têm uma redução de 25 % sobre o montante das taxas aplicáveis, sendo a verificação da qualidade de PME efetuada pelo GNS através da consulta da certificação PME no sítio na Internet do IAPMEI, conforme nº 2 do artigo 4º da mesma Portaria.

2.10. Reconhecimento e transferência de certificados

O presente Esquema permite o reconhecimento de certificados de outros organismos de certificação, reservando-se, no entanto, o GNS o direito de verificar, no todo ou em parte, a conformidade dos produtos certificados por outras entidades relativamente ao presente Esquema.

Em função do resultado da verificação, o GNS pode conferir o reconhecimento do certificado, ou informar a EReq dos procedimentos a adotar para esse fim.

2.11. Ciclo de revisão

Salvo disposição em contrário o presente Esquema, deve ser revisto a cada três anos e sempre que se considerar necessário.

3. Processo de avaliação da conformidade

O processo de avaliação da conformidade compreende, genericamente:

- Fase do pedido de avaliação;
- Fase da avaliação técnica;
- Fase do relatório de avaliação técnica (RAT).

Os prazos indicados nesta secção são tempos médios expetáveis e indiciadores de um bom serviço.

3.1. Fase do pedido de avaliação

A EReq deve proceder ao pedido de avaliação junto do OAV, através do envio/preenchimento do formulário de pedido[7] com a informação indicada no Anexo A.

[7] Todas as notificações, comunicações, fundamentações e argumentações referidas serão efetuadas preferencialmente por via eletrónica.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Após a receção do pedido de avaliação nos termos referidos no parágrafo anterior, o OAV deve proceder à análise do mesmo e, caso seja necessário, deve marcar uma reunião para clarificar:

- A documentação a ser entregue;
- A concretização dos requisitos de admissão ao Esquema;
- A definição do perfil de proteção, nível de garantia e estimativa de esforço;
- O estabelecimento de um Acordo de Confidencialidade e clarificação sobre a propriedade intelectual (modelo no anexo H);
- A entrega de amostras do produto;
- A definição do Plano de Avaliação;
- O contrato de Avaliação.

Caso não se encontrem reunidos os requisitos para proceder à avaliação do produto, o OAV deve notificar a EReq para remeter documentação adicional ou os esclarecimentos necessários, para que seja possível prosseguir com o pedido.

Após os requisitos para proceder à avaliação do produto se encontrarem reunidos, o OAV deve enviar, no prazo de 15 dias úteis, uma proposta contratual para realizar a avaliação à EReq, contendo os direitos, deveres e responsabilidades de cada uma das partes, assim como, a da equipa de avaliação, a quantidade de horas necessárias para realizar a avaliação e o respetivo encargo financeiro.

É responsabilidade da EReq entregar ao OAV toda a informação necessária sobre o produto para o qual requer a avaliação, bem como permitir o acesso a documentos, avaliações subcontratadas, registos, pessoal, produtos, serviços, instalações e outros que se considerem relevantes para o objetivo e âmbito da avaliação técnica.

O contrato entre as partes deve definir as condições para a disponibilização do produto alvo do pedido de avaliação.

3.2. Fase da avaliação técnica

A entrega do produto ao OAV marca o início da fase de avaliação técnica, devendo o OAV notificar o GNS acerca do calendário dos ensaios ou inspeções a realizar. O GNS reserva-se o direito de estar presente durante estas atividades, podendo intervir na eventual seleção ou recolha de amostras por parte do OAV, bem como verificar as condições em que estas atividades são efetuadas e os respetivos registos e arquivos.

A avaliação técnica pode ser de três tipos:

- Inicial – quando o produto nunca foi certificado.
- Extraordinária – quando um produto certificado sofre alguma alteração significativa na sua configuração, ou quando os normativos aplicáveis se alteraram e requerem nova avaliação do produto certificado.
- Recertificação - quando expirou o prazo de certificação e se pretende renovar a certificação do produto.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Os diferentes tipos de avaliação técnica têm por objetivo aferir o cumprimento da implementação dos requisitos de segurança em função de um referencial específico, de acordo com os métodos de verificação e tendo em atenção o nível de garantia pretendido pela EReq, devendo ter em conta os seguintes princípios:

- Adequação - As atividades de avaliação efetuadas para atingir um dado nível de garantia pretendido devem estar de acordo com as melhores práticas, devendo ainda empregar uma linguagem clara e de fácil entendimento por todas as partes envolvidas nas atividades de avaliação e certificação.
- Imparcialidade - Todas as avaliações devem estar isentas de quaisquer pressões comerciais, financeiras ou outras influências que possam favorecer ou prejudicar o resultado da decisão com base em valorações subjetivas ou opções arbitrárias.
- Objetividade - Os resultados da avaliação devem claros e precisos e conter todos os elementos considerados adequados e necessários para o completo esclarecimento do resultado da avaliação, evitando a subjetividade e a opinião.
- Repetibilidade e reprodutibilidade – Uma avaliação de poder ser repetida para um mesmo equipamento ou produto, com os mesmos requisitos e com a mesma evidência de avaliação, e produzir um resultado igual.
- Solidez dos resultados - O resultado de cada avaliação deve ser coerente, completo e tecnicamente correto por forma a promover a confiança na segurança dos produtos certificados sob este Esquema.
- Comparabilidade – O resultado de cada avaliação deve, salvo casos devidamente justificados, ser comparável com os de outras instituições ou organizações internacionais idóneas.
- Usabilidade – A metodologia empregue na avaliação deve estar alinhada com os diferentes fatores ambientais e/ou técnicos que uma exploração normal acarreta.
- Eficiência - O valor de uma avaliação deve compensar o tempo, os recursos e o investimento feito por todos os intervenientes.

O OAV procede à avaliação técnica e à elaboração do respetivo relatório, no qual deve registar as não conformidades (NC) detetadas no decurso da avaliação.

A avaliação inicial tem por objetivo validar todos os requisitos de acesso e de implementação de um perfil de proteção devidamente definido e aprovado, podendo sugerir ajustes para aprovação pelo GNS.

A avaliação extraordinária tem por objetivo validar a implementação de ações corretivas, para avaliar alterações no âmbito de uma certificação já conferida a um produto ou para efeitos de reconhecimento de outras avaliações. As avaliações extraordinárias não substituem as avaliações previstas no ciclo de certificação.

A avaliação de recertificação é realizada a pedido da EReq, com pelo menos 4 meses de antecedência relativamente ao termo do prazo de validade do certificado de certificação.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Os OAV podem considerar a informação relativa a outros processos de avaliação desenvolvidos para o mesmo produto, assim como relatórios de avaliação e certificados de conformidade no âmbito de outros processos de certificação similares.

3.3. Equipa de avaliação técnica

As equipas de avaliação técnica devem ser compostas por elementos com competência técnica e experiência profissional adequadas para realizar as avaliações e serem possuidores de credenciação de segurança na marca Nacional conferida pela ANS no grau de segurança mínimo ao grau do produto em avaliação.

Com exceção para os Laboratórios acreditados pelo IPAC, os OAV devem garantir que pelo menos um elemento da equipa de avaliação técnica, cumpra os seguintes requisitos:

- Capacidade de gerir a equipa (líder da equipa);
- Possuir conhecimento comprovado dos requisitos legais e regulamentares, incluindo na área específica de segurança da informação;
- Possuir conhecimento comprovado do estado da arte da certificação de produtos;
- Possuir conhecimento comprovado em tecnologias e metodologias aplicáveis na avaliação do produto auditado;
- Possuir conhecimento comprovado da realização de avaliação do risco no âmbito da segurança da informação para identificar ativos, ameaças e vulnerabilidades em produtos e compreender seu impacto, mitigação e controlo;
- Possuir conhecimento para rastrear possíveis indicações de incidentes de segurança até aos elementos apropriados de controlo do produto;
- Ter atuado como auditor ou ter participado em, pelo menos, dois ou mais processos de avaliação técnica;
- Possuir conhecimentos e atributos adequados para gerir o processo de avaliação.

Os especialistas técnicos que integram a equipa de avaliação técnica cumprir os seguintes requisitos:

- Conhecimento dos requisitos legais e regulamentares e de conformidade legal no campo específico da segurança da informação;
- Conhecimento comprovado do estado da arte atual da certificação e produtos;
- Conhecimento comprovado em tecnologias aplicáveis na avaliação do produto auditado;
- Conhecimento comprovado na realização de avaliação do risco relacionado com a segurança da informação para identificar ativos, ameaças e vulnerabilidades em produtos e compreender seu impacto, mitigação e controlo;
- Conhecimento de análise de vulnerabilidades de segurança de rede, incluindo testes de penetração;
- Conhecimento de avaliação de controlos de segurança; e
- Conhecimento de avaliação de produtos (por exemplo, conforme ISO/IEC 15408 [i.7]), devendo ser capaz de avaliar a operação segura de produtos avaliados ou sistemas confiáveis, como módulos criptográficos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Uma equipa técnica deve ser constituída, no mínimo, por 2 elementos.

Uma avaliação técnica não deve exceder os 60 dias seguidos, nem possuir menos de 120horas/pessoa, devendo o OAV documentar e justificar o tempo utilizado no relatório de avaliação técnica.

3.5. Fase do Relatório de Avaliação Técnica (RAT).

Após a realização e conclusão da avaliação técnica, o OAV deve apresentar o respetivo RAT, no prazo de 10 dias úteis.

O RAT deve ser suficientemente detalhado para facilitar e apoiar uma decisão sobre uma candidatura à certificação, por parte do OCC, devendo conter as seguintes informações:

- Resumo da revisão dos documentos e das normas, especificações disponíveis e/ou requisitos legais e regulamentares em relação aos quais a avaliação é realizada;
- As áreas cobertas pela avaliação, incluindo os requisitos de avaliação, os ensaios e as metodologias de avaliação utilizadas;
- Análise do risco de segurança da informação manuseada pelo produto;
- Evidenciar a forma como o produto cumpre e mantém o controlo de versões ao longo do seu ciclo de vida;
- As observações feitas, tanto positivas quanto negativas;
- Os detalhes de quaisquer não conformidades identificadas, apoiadas por evidências objetivas (se aplicável) e uma referência única ao requisito que não foi atendido;
- Os mecanismos de segurança de cada produto implementados por defeito e os opcionais, e o nível de proteção oferecido pelo produto avaliado;
- Tempo total de avaliação usado e especificação detalhada do tempo gasto na revisão de documentos, avaliação do produto, avaliação e análise dos riscos e relatórios de auditoria;
- Os comentários sobre a conformidade do produto com os critérios pelos quais a avaliação foi realizada, juntamente com uma declaração clara de não conformidade e, quando aplicável, qualquer comparação útil com os resultados de avaliações anteriores ao produto em causa;
- Inquéritos/entrevistas efetuadas, justificativas para sua seleção e a metodologia empregue, incluindo metodologia de amostragem e procedimentos de teste;
- Parecer técnico quanto ao cumprimento dos requisitos do presente Esquema.

Os questionários preenchidos, listas de verificação, observações, registos ou notas de avaliação devem fazer parte integrante do RAT, como anexos.

De modo a uniformizar a elaboração do RAT, o OAV deve observar o modelo geral que consta do Anexo J, de modo a garantir que são fornecidos ao GNS os detalhes suficientes para demonstrar adequadamente a avaliação técnica realizada.

O RAT é redigido em português, podendo ser redigido em inglês desde que devidamente justificado.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

O RAT deve ser assinado digitalmente, com assinatura digital qualificada, pelo chefe da equipa de avaliação técnica, com o atributo da data visível.

3.5.1. Ações corretivas

O OAV deve informar a EReq de todas as NC presentes no RAT, parametrizando risco associado e identificando as respetivas ações corretivas.

3.5.2. Nível de proteção

Todos os produtos devem apresentar uma configuração de segurança que proteja a informação contra múltiplas ameaças. A avaliação da conformidade em Segurança Tecnológica visa distinguir o investimento na segurança e na inovação, sendo necessário caracterizar os produtos que oferecem um melhor nível de proteção.
Neste sentido, o nível de proteção visa assegurar a implementação do conceito "*Security by Default*". A sua fórmula de cálculo está apresentada nas definições <Nível de proteção>.

Os mecanismos de proteção de cada produto apenas podem ser quantificados uma única vez, não sendo consideradas as múltiplas opções de configuração existentes para um mesmo mecanismo.

No Anexo F ao presente Esquema consta uma lista exemplificativa de mecanismos de proteção passiveis de serem usados como requisitos do produto para os diferentes tipos de produtos.

3.5.3. Níveis garantia de segurança

A avaliação de produtos compreende três níveis de garantia de segurança – **"BÁSICO", "MELHORADO" e "SUPERIOR",** permitindo que cada EReq selecione o nível de garantia mais adequado para o seu produto, em função do contexto em que se insere, assim como, facilitar o desenvolvimento faseado do seu produto em função da respetiva maturidade.

Desta forma, o presente Esquema pretende possibilitar que todas os interessados, independentemente da sua dimensão, possam alcançar uma certificação para os seus produtos, de acordo com a qualidade dos mesmos nos parâmetros avaliados, permitindo ainda dispor de um Esquema que lhes apresente oportunidades de melhoria contínua.

Os requisitos de segurança definidos para cada um dos níveis de garantia de segurança seguem uma lógica sequencial e evolutiva.

Compete à ANS definir, para cada TIC passível de ser certificada pelo presente Esquema, os respetivos níveis de garantia de segurança admissíveis em função da maturidade e do risco que a utilização de determinada tecnologia representa para a IC.

3.5.4. Resultado global da avaliação

O resultado global da avaliação tem por base o nível de proteção, o nível de garantia de segurança e os demais requisitos de avaliação, devendo o OAV emitir um parecer global sobre os resultados alcançados pelo produto avaliado e as possíveis vulnerabilidades identificadas no RAT.

3.6. Métodos e critérios de avaliação

O nível de conformidade de cada produto é determinado por um conjunto de requisitos designados por perfil de proteção.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Os perfis de proteção são específicos para cada classe de produto, e estão apresentados nos anexos B, C, D e E, que se constituem como requisitos iniciais para a Certificação.

3.7. Controlo de versões do produto sujeito a avaliação

A EReq deve registar todas as atualizações realizadas aos produtos certificados, sendo que, quando as alterações corresponderem a uma nova versão do produto, o mesmo deve ser alvo de uma avaliação extraordinária.

No âmbito da gestão de produtos são passíveis de notificação todas as alterações ocorridas a uma configuração testada que tenham por base uma correção.

Todas as alterações realizadas em versões associadas a alterações de sistema operativo, interface de programação da aplicação (API), mudança de bibliotecas e quaisquer alterações que afetem a compatibilidade binária do produto ou mecanismos de segurança, devem ser alvo de uma avaliação extraordinária.

As alterações relacionadas com a correções de bugs e vulnerabilidades devidamente identificadas e referenciadas que mantêm a compatibilidade com as versões anteriores, não carecem de uma nova avaliação.

Sempre que subsistirem dúvidas, compete ao OCC aferir se uma alteração carece de ser novamente avaliada ou não.

3.8. Reclamações

Eventuais reclamações sobre qualquer decisão por parte do OAV e reclamações relativas ao processo de avaliação devem ser endereçadas ao OAV.

Caso não sejam passiveis de ser ultrapassadas as divergências entre a EReq e o OAV, podem ser endereçadas reclamações ao OCC.

3.9. Conservação de registos pelos organismos de avaliação da conformidade

O OAV deve manter um sistema de registos de acordo com os requisitos da norma de acreditação ISO / IEC 17020 ou ISO / IEC 17025.

O sistema de registos deve incluir todos os registos e outros documentos produzidos em relação a cada avaliação de conformidade, bem como documentos e evidências fornecidas pela EReq sobre a implementação de requisitos de segurança. Deve ainda incluir uma lista dos documentos e evidências disponibilizados apenas temporariamente pela EReq durante a avaliação da conformidade. O sistema de registos deve ser suficientemente completo para permitir que o curso de cada processo de certificação seja replicável.

3.10. Dever de informação do OAV para com o OCC

É responsabilidade do OAV informar o GNS do seguinte:

- Desajustes observados de perfis de proteção constantes no Esquema, podendo propor alterações/correções/adições a esses perfis, desde que devidamente justificadas;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- Necessidade de desenvolvimento de novos perfis de proteção para tecnologias especificas, dando conta dos pedidos recebidos, assim como, do impacto do novo perfil no presente Esquema;
- Alterações no âmbito dos produtos certificados;
- Medidas tomadas para resolver anomalias identificadas nos procedimentos internos;
- Alterações do respetivo estatuto legal e organizacionais, incluindo alterações de designação legal e transferência de direitos de propriedade sobre serviços prestados, mudança de instalações, ou de composição das equipas de avaliação técnica.
- Alterações de elementos de contacto.

4. Processo de certificação da conformidade

O processo de certificação da conformidade inicia-se após conclusão do processo de avaliação, sendo composto pelas seguintes fases:

- Fase de preparação da documentação (elaboração do plano de ações corretivas e do Manual de Procedimentos de Segurança);
- Fase de candidatura à certificação;
- Fase de apreciação e decisão de certificação;
- Fase de acompanhamento da certificação.

O OCC reserva-se do direito de recusar serviços com entidades sobre as quais existam razões fundamentadas que impactem negativamente na imagem e reputação do OCC. Encontram-se nestas circunstâncias, entre outras, as entidades que desenvolvam atividades ilegais ou que apresentem um historial de não cumprimento com os requisitos de certificação.

4.1. Fase de preparação da documentação

A EReq deve desenvolver um Plano de Ações Corretivas identificando, para cada NC identificada no RAT, as causas, as ações corretivas e o prazo para a respetiva implementação.

O prazo de implementação das ações corretivas, incluindo o envio das respetivas evidências, não deve exceder 3 meses, podendo em situações de extrema complexidade comprovada ser estendido até 12 meses, após aprovação do OCC.

A EReq deve também desenvolver um Manual de Procedimentos de Segurança que identifique o produto, a configuração avaliada com sucesso e os principais procedimentos que contribuem para que o produto se mantenha numa configuração de "*Security by Default*".

O Manual de Procedimentos de Segurança (SecOPS) deve incluir informação referente a:

- Âmbito;
- Contexto de utilização;
- Descrição e características gerais do produto;
- Diferentes configurações do produto;
- Arquitetura Física do produto;
- Arquitetura Lógica produto, se aplicável;
- Arquitetura Aplicacional do produto, se aplicável;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- Fluxos de informação gerais do produto, se aplicável;
- Serviços disponibilizados pelo produto, se aplicável;
- Requisitos mínimos de Hardware/Software, se aplicável;
- Requisitos mínimos de cablagem e bastidor, se aplicável;
- Contexto do utilizador;
- Contexto de administração;
- Contexto de desenvolvimento, se aplicável;
- Documentação disponível para consulta geral;
- Definição de procedimentos de instalação e acesso;
- Definição de procedimentos de configuração;
- Definição de procedimentos de criação de utilizadores, de administradores e de auditores de segurança, se aplicável;
- Definição de procedimentos de exploração, registo e arquivo de dados, se aplicável;
- Definição de procedimentos de controlo de configuração;
- Definição de procedimentos de manutenção de segurança;
- Definição de procedimentos de manutenção criptográfica, se aplicável;
- Definição de procedimentos de auditoria e análise de vulnerabilidades;
- Definição de procedimentos de cópia, transferência ou extração de dados, se aplicável;
- Definição de procedimentos de utilização de outras aplicações externas, se aplicável;
- Definição de procedimentos de utilização de periféricos e dispositivos amovíveis de memória, se aplicável;
- Definição de procedimentos de copia de segurança, se aplicável;
- Definição de procedimentos de reporte de incidente ou vulnerabilidade;
- Definição de procedimentos de aviso de novas versões do produto;

4.2. Fase de candidatura à certificação

A EReq formaliza a sua candidatura através do preenchimento e envio de um formulário (Anexo K), enviando também o Plano de Correções e o Manual de Procedimentos de Segurança.

> **Nota:** O mesmo procedimento é aplicado caso a EReq pretenda a alteração de uma certificação em vigor para um diferente nível de garantia do presente Esquema. Nesta situação, o GNS avalia a necessidade de ser realizada uma avaliação extraordinária para esse efeito.

Caso a informação disponibilizada não esteja conforme, o GNS deve notificar a EReq, no prazo de 10 dias úteis, para a entrega de documentação adicional ou os esclarecimentos necessários para que seja possível prosseguir com a candidatura.

Quando a informação disponibilizada estiver conforme, o GNS notifica, no prazo de 10 dias úteis, a EReq da sua aceitação da candidatura.

Apenas serão aceites processos de candidatura com RAT válido e emitido no prazo máximo de 12 meses, em relação à apresentação da candidatura no sítio da Internet do GNS.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

O GNS pode proceder ao encerramento da candidatura, notificando a entidade responsável, caso o mesmo não responda às suas solicitações após um período de 3 meses.

As candidaturas só serão aceites se a informação prestada pela EReq estiver completa.

4.3. Fase de apreciação e decisão de certificação

Após análise e aceitação da candidatura, o OCC, dispõe de um período de 45 dias para apreciar a candidatura, analisar a documentação submetida, e estabelecer as condições para a certificação, em caso de aprovação.

A entidade EReq deve estar disponível para a realização de reuniões com o OCC, permitir o acesso a documentos, registos, avaliações subcontratadas, pessoal, produtos, serviços, instalações e outros que se considerem relevantes para o objetivo e âmbito da certificação.

O OCC, após analise do relatório de avaliação técnica, deve proceder à respetiva decisão de certificação no prazo máximo de 5 dias úteis.

É tomada a decisão de emissão do certificado quando:

- Foi observada a conformidade para com o perfil de proteção;
- Foi estabelecido um nível de proteção oferecido pelo produto candidato;
- Foi estabelecido um nível de garantia oferecido pela avaliação realizada;
- As criticidades das vulnerabilidades são conhecidas;
- As ações corretivas propostas pela entidade responsável encontram-se implementadas com uma eficácia comprovada;
- As não conformidades do produto encontram-se resolvidas e garantem o cumprimento dos requisitos;
- Os procedimentos de segurança dão conta de que o produto segue os princípios de *Security by Design* e *Security by Default*, tendo o risco residual sido identificado e tratado por via de procedimentos ou processos alternativos, mas devidamente descritos.

Em caso de decisão positiva, o GNS emite o Certificado de Conformidade e estabelece uma relação entre o nível de garantia e o grau de informação classificada que o produto se encontra habilitado a manusear, podendo ser[8]:

- Nível **"BÁSICO"**, para IC com o grau de segurança **RESERVADO;**
- Nível **"MELHORADO"**, para IC com o grau de segurança **CONFIDENCIAL;**
- Nível **"SUPERIOR"**, para IC com o grau de segurança **SECRETO.**

A validade máxima do certificado de conformidade é de 36 meses.

[8] Foi tomado por base o alinhamento proposto pelos documentos: AC/322-D(2006)0006 - Directive on the use of the Common Criteria Within NATO e AC/322-D(2005)0043 - Directive for the Assessment of Assurance Levels in Specific CIS Environments;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

No caso de decisão de não conferir a certificação, a ANS fundamenta a sua decisão e notifica-a ao EReq.

A certificação concedida só é válida para o produto indicado no certificado de conformidade, não podendo a EReq transmitir ou associar a certificação a outros produtos. A referência ou declaração relativamente à certificação não deve permitir qualquer entendimento que seja falso ou se preste a mal-entendidos sobre a correta identificação do produto certificado.

No decurso da renovação da certificação será aferida a utilização da etiqueta de certificação e do certificado de conformidade, havendo lugar ao registo de não conformidades, caso se detete a utilização indevida ou o incumprimento das regras estabelecidas.

A suspensão, anulação ou revogação ou não atribuição da certificação implica a cessação imediata da utilização do certificado de conformidade do produto pela EReq.

4.4. Fase do acompanhamento da certificação

Cerca de 4 meses antes do fim do prazo de certificação de um produto, assumindo a intenção que a mesma seja renovada, inicia-se uma ação de renovação de certificação.

Durante esta fase, a EReq deve comunicar ao GNS qualquer alteração relevante que possa afetar a certificação conferida, nomeadamente:

- Alterações de estatuto legal e organizacionais, incluindo da designação legal e transferência de direitos de propriedade sobre produtos certificados;
- Alterações de elementos de contacto;
- Alterações no âmbito dos produtos certificados;
- Vulnerabilidades descobertas após certificação do produto;
- Medidas tomadas para resolver anomalias e vulnerabilidades identificadas;
- Alteração ao processo de tratamento de anomalias, vulnerabilidades ou anúncio das mesmas.

O GNS decidirá da necessidade de realização de uma avaliação extraordinária para avaliar as alterações reportadas.

O GNS pode realizar ações de avaliação extraordinária durante o período de validade da certificação do produto, sempre que considerar necessário ou adequado.

Os lançamentos de novas versões do produto invalidam a certificação de conformidade e o respetivo certificado. Caso se pretenda manter a certificação, a EReq deve solicitar nova avaliação para fins de certificação, junto do OAV.

4.5. Suspensão e anulação da certificação

O OCC pode tomar a decisão de suspensão da certificação quando:

- Não seja comunicado ao OCC incidente de segurança ocorrido no prazo estipulado no certificado do produto;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- Não sejam comunicadas ao OCC quaisquer vulnerabilidades de nível crítico ou elevado, de acordo com a versão mais recente do referencial *Common Vulnerability Scoring System* (CVSS);
- Não seja possível, por causa imputável à EReq, a realização de quaisquer avaliações determinadas pelo OCC;
- A EReq não dê resposta aos RAT e/ou não evidencie a implementação das ações corretivas desencadeadas na sequência das avaliações dentro dos prazos previstos e/ou determinados pelo OCC;
- A EReq não dê resposta às demais solicitações do OCC;
- O RAT de uma avaliação extraordinária ou de recertificação evidenciar não estarem reunidas os requisitos para a manutenção da certificação;
- Seja detetado qualquer incumprimento relativo à utilização do certificado de conformidade e/ou da marca e etiqueta de certificação;
- Sejam evidenciados atos que sejam lesivos para a imagem do OCC e/ou do(s) proprietário(s) da marca e etiqueta de certificação;
- Ocorram incumprimentos de obrigações de ordem financeira para com o OCC por parte da EReq.

A suspensão da certificação deve ser levantada quando se demonstrar que a causa que esteve na origem da suspensão da certificação já não existe. O levantamento da suspensão da certificação pode ser efetuado através da análise de evidências documentais, quando suficiente, ou através de uma avaliação extraordinária.

Após o levantamento da suspensão, o ciclo de certificação é retomado, mantendo-se a data de validade original do certificado de conformidade.

A suspensão da certificação pode ter uma duração máxima de 12 meses.

Quando não seja possível proceder ao levantamento da suspensão da certificação, a ANS procede à anulação da certificação.

4.6. Reclamações e recursos

Eventuais recursos sobre qualquer decisão por parte do OCC e reclamações relativas ao OCC devem ser endereçados à Autoridade Nacional de Segurança.

4.7. Conservação de registos pelos organismos de certificação

O OCC deve manter um sistema de registos de acordo com os requisitos da norma de acreditação ISO / IEC 17065.

O sistema de registos deve incluir os registos e outros documentos produzidos em relação a cada certificação da conformidade, bem como documentos e evidências fornecidas pela EReq sobre a implementação de requisitos de segurança. Deve ainda incluir uma lista dos documentos e evidências disponibilizadas pela EReq durante a avaliação da conformidade. O sistema de registos deve ser suficientemente completo para permitir que o curso de cada processo de certificação seja replicável.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Todos os registos devem ser armazenados de forma segura e acessível por um período mínimo de (5) anos após a cessação da vigência do certificado.

4.8. Conteúdo e formato dos certificados

O certificado segue o modelo apresentado no anexo L, e inclui:

- Um identificador único atribuído pelo GNS;
- Nome da EReq (e eventual o sítio web);
- Assinatura digital qualificada por parte do ANS;
- Nome e informação de contacto do OAV;
- Referência ao presente Esquema, com identificação da versão utilizada;
- Grau de certificação atribuído;
- Identificação do produto certificado;
- Limites à certificação, caso existam;
- Data de emissão e a data de validade do certificado;
- A etiqueta e marca .

4.11. Política de divulgação dos certificados

A política de divulgação de certificados do esquema de certificação em Segurança Tecnológica assenta na transparência, pelo que todos os certificados emitidos pelo GNS podem ser consultados no portal a Internet do GNS.

A EReq, após conclusão do processo de certificação com sucesso, também pode publicar no seu portal o referido certificado ou criar uma hiperligação para o portal do GNS.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

5. Processo de constituição de organismos de avaliação da conformidade (OAV)

Qualquer entidade estabelecida em Portugal que pretenda candidatar-se a ser Organismos de Avaliação de conformidade, deve solicitar essas intenções junto do Gabinete Nacional de Segurança.

Os OAV são constituídos por Laboratórios, por Organismos de Inspeção ou por pessoa singular ou coletiva.

Tanto os Laboratórios como os Organismos de Inspeção (OI) devem estar previamente acreditados pelo Instituto Português de Acreditação (IPAC), de acordo com as normas ISO/IEC 17025 (Labs.) e ISO/IEC 17020 (OI).

O presente Esquema possui requisitos de confidencialidade, independência e imparcialidade, podendo o IPAC definir requisitos adicionais para a acreditação dos OAV.

5.1 Documentação obrigatória

A entidade candidata tem de fornecer a seguinte documentação:

a) Certidão de credenciação industrial válida, obtida junto do GNS;
b) Certificado de acreditação como organismo de avaliação da conformidade, emitido pelo IPAC;
c) Certificado de acreditação de segurança da informação classificada, emitido pelo GNS, para o sistema de informação e de comunicação a ser utilizado para a realização de testes e avaliações técnicas;
d) Estatutos da pessoa coletiva e tratando-se de sociedade o contrato de sociedade ou, tratando-se de pessoa singular, a respetiva identificação e domicílio;
e) Tratando-se de sociedade, a relação de todos os sócios, com especificação das respetivas participações, bem como dos membros dos órgãos de administração e de fiscalização, e, tratando-se de sociedade anónima, a relação de todos os acionistas com participações significativas, diretas ou indiretas;
f) Declarações subscritas por todas as pessoas singulares e coletivas referidas de que não se encontram em nenhuma das situações indiciadoras de falta de idoneidade;
g) Comprovativo de contrato de seguro válido para cobertura adequada da responsabilidade civil emergente do exercício de atividade comercial, como organismo de avaliação da conformidade;
h) Política de prestação do(s) serviço(s) de avaliação para os quais é solicitada a candidatura;
i) Descrição da capacidade para efetuar ensaios/testes de todos os esquemas para o qual o estatuto qualificado é solicitado;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

j) Uma cópia do contrato padrão a disponibilizar no âmbito da prestação de serviços de avaliação da conformidade;
k) Uma cópia do acordo de confidencialidade padrão a disponibilizar (*end-user agreement*), no âmbito da prestação de serviços de avaliação da conformidade;
l) Uma cópia do relatório padrão de avaliação técnica (RAT) a disponibilizar no âmbito da prestação de serviços de avaliação da conformidade;
m) Cópia de todos os contratos de prestação de serviços com entidades externas (terceiros) que contribuam direta ou indiretamente para a prestação de serviços de avaliação da conformidade;
n) Identificação dos auditores e da sua credenciação individual;
o) Declaração do nível de habilitação, formação e experiência do líder da equipa de avaliação;
p) Declaração do nível de habilitação, formação e experiência dos restantes auditores da equipa de avaliação;

Esta documentação deverá ser enviada juntamente com o formulário de Candidatura de Organismos de Avaliação da Conformidade (Anexo I), devidamente preenchido, assinado e endereçado ao GNS através do endereço de correio eletrónico: dsdti.st@gns.gov.pt .

O comprovativo de pagamento das taxas aplicáveis deverá ser remetido pelo mesmo endereço.

Após análise da candidatura, e caso sejam cumpridos os requisitos necessários, é atribuído o estatuto de OAV pela ANS.

Os OAV apenas podem exercer o serviço de avaliação técnica da conformidade depois de estarem autorizados para o efeito pela ANS e o respetivo estatuto de OAV estar publicado no portal do GNS na lista de OAV nacionais.

5.3. Requisitos de Confidencialidade

O presente Esquema assenta em requisitos de confidencialidade que visam mitigar o risco de informação proprietária ou sujeita a direitos de autor ser mal manuseada ou tornar-se do conhecimento de entidades não envolvidas no processo de avaliação e de certificação.

Os requisitos de confidencialidade assentam na elaboração de um acordo de confidencialidade, assim como no estabelecimento, em caso de necessidade, de canais de comunicação específicos e dedicados através de plataformas de qualquer uma das entidades envolvidas.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

5.4. Requisitos de Independência e Imparcialidade

O presente Esquema assenta em requisitos de independência e imparcialidade, que visam evitar que o processo de avaliação técnica possa ser desvirtuado ou sofrer de outras intenções que não sejam a segurança dos produtos avaliados.

Para evitar as pressões comerciais, financeiras ou outras que possam comprometer qualquer avaliação, é mandatório que:

- Os elementos de uma equipa de avaliação técnica não podem ter participado ou tido influência sobre a conceção, desenvolvimento, desenho, produção, distribuição, venda, instalação ou manutenção de um produto sujeito a avaliação, há menos de 2 anos;
- Os elementos da equipa técnica de avaliação devem assinar, individualmente, uma Declaração de Inexistência de Conflitos de Interesse, em relação à entidade que apresenta a candidatura;
- O OAV não pode avaliar produtos produzidos pela própria entidade legal;
- A entidade legal na qual se insere o OAV apenas pode comercializar produtos certificados, se existirem as condições mínimas que garantam a imparcialidade e os seus produtos tenham sido avaliados por um OAV com entidade legal distinta;
- Os OAV que se candidatem a avaliação de produtos criptográficos e de baixa radiação (TEMPEST) devem possuir independência total perante o tipo de produto sujeito a avaliação, ou seja, a entidade legal em que se insere o OAV, bem como os elementos da equipa de avaliação técnica não podem ter participado no seu desenvolvimento, conceção, desenho, produção, distribuição, venda, instalação ou manutenção.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO A – Formulário de pedido de avaliação ou alteração a pedido realizado

O pedido de avaliação de conformidade ou alteração ao mesmo é realizado online, no sítio da Internet do OAV, através do preenchimento de um formulário e junção de documentação identificada, no sentido de permitir recolher informação necessária para dar início ao processo respetivo.
O site online deve ter a opção de uploads de ficheiros em formato pdf com tamanho, pelo menos, de 20 MB, para submissão da documentação.

O formulário disponível online deverá ter a seguinte estrutura:

Secção 1: Identificação do produto candidato.

Esta secção deve incluir toda a informação relevante do produto proposto para avaliação.

- Identificação da entidade responsável: (Nome, número de identificação fiscal e morada da sede).
- Contacto da entidade: (Identificação do ponto de contacto da entidade que irá ser responsável pelo acompanhamento do processo de avaliação).
- Identificação do produto candidato: (Nome do produto).
- Descrição sumária do produto ou das alterações em relação às informações previamente facultadas que dizem respeito à caracterização do produto avaliado.
- Nível de garantia (Nível de garantia para a qual o produto se pretende candidatar a avaliação: "Básico", "Melhorado" ou "Superior".
- Tipo de atividade associada à avaliação: Pedido de avaliação, alteração da avaliação, avaliação extraordinária, etc.

Secção 2: Declaração de compromisso

Deverá ser datada e assinada e deve pelo menos confirmar:

- Que a documentação reflete as funções, os processos, os procedimentos e os componentes usados.
- Que a documentação para a avaliação se encontra disponível.
- Que a organização e o seu responsável se comprometem a cumprir todas as obrigações decorrentes do presente Esquema durante a avaliação e após a obtenção da certificação durante o período de validade da certificação.
- O responsável pela entidade declara que é responsável pelos pontos acima mencionados.

Secção 3: Comprovativo de cumprimento dos requisitos gerais de admissão

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Deve descrever ou evidenciar a forma como o produto cumpre os requisitos gerais de admissão ao Esquema de Certificação em Segurança Tecnológica.

Sobre o produto, apresentar a seguinte informação:

- Contexto de utilização;
- Descrição e características gerais do produto;
- Referenciais usados, assim como, outras avaliações / certificações efetuadas;
- As suas possíveis configurações;
- Arquitetura Física;
- Arquitetura Lógica;
- Arquitetura Aplicacional;
- Fluxos gerais de informação;
- Serviços disponibilizados pelo produto;
- Versões de sistema operacional suportadas;
- Descrição do controlo de versões do produto;
- Intervalo temporal entre atualizações;
- Requisitos mínimos de Hardware/Software;
- Contexto do utilizador;
- Contexto de administração;
- Mecanismos de segurança do produto (com informação sobre os que se encontram ativados por defeito ou por opção);
- Componentes;
- Componentes importantes, mas que não fazem parte do produto;
- Dependências de terceiros;
- Documentação disponível para consulta geral;

No caso de se tratar de uma alteração, descrição das alterações às informações previamente facultadas que dizem respeito à caracterização do produto certificado.

Secção 4 - Declaração de sigilo comercial

Deverá ser identificada a informação que no âmbito do processo de avaliação, são considerados sujeitos a sigilo comercial ou protegidos por direitos de propriedade intelectual ou industrial.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO B – Requisitos para Produtos Comerciais não Criptográficos

B.1. Requisitos do produto

Os produtos devem ser concebidos, desenvolvidos e produzidos de forma a garantir um nível adequado de segurança com base no conceito "*Security by Design*".

Devem ainda ser entregues com uma configuração padrão segura "*Security by Default*", incluindo a possibilidade de voltar ao seu estado original e sem quaisquer vulnerabilidades exploráveis conhecidas, pelo que se constituem como requisitos do produto (mecanismos de segurança) a observar em cada produto:

Grupo de Mecanismos	Nome do Grupo	MS ID	Mecanismo de Segurança	Dispositivo			Aplicação		
				Básico	Melhorado	Superior	Básico	Melhorado	Superior
GM01	Auditoria de Segurança	MS01	Análise da Cadeia de Abastecimento		X	X		X	X
		MS02	Análise de Conteúdo			X			X
		MS03	Análise de Conformidade			X			X
		MS04	Análise de Integridade de dados	X	X	X	X	X	X
		MS05	Análise de Registos	X	X	X	X	X	X
		MS06	Análise de Vulnerabilidades			X			X
GM02	Identificação, Autenticação e Autorização de acesso	MS07	Identificação e Autenticação	X	X	X	X	X	X
		MS08	Autorização	X	X	X	X	X	X
		MS09	Certificados digitais			X			X
		MS10	Assinaturas digitais			X			X
		MS11	Infraestrutura de Chaves Públicas			X			X
GM03	Integridade	MS12	Proteção de Integridade de Hardware	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS13	Proteção da Configuração de Hardware	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS14	Proteção da Configuração de Sistema Operativo		X	X		X	X
		MS15	Proteção da Configuração de Aplicações		X	X		X	X
		MS16	Proteção de Bibliotecas de Software/Firmware	X	X	X	X	X	X
		MS17	Proteção de Código			X			X
		MS18	Proteção de Dados		X	X		X	X
GM04	Disponibilidade	MS19	Proteção Anti-roubo	X	X	X		X	X
		MS20	Falha Segura	X	X	X		X	X
		MS21	Operação em ambiente degradado	X	X	X		X	X
		MS22	Proteção contra Denial of Service	X	X	X	X	X	X
		MS23	Proteção contra Malware	X	X	X	X	X	X
GM05	Comunicações	MS24	Proteção de Ethernet		X	X		X	X
		MS25	Proteção de Wireless		Não Aplicável	Não Aplicável		Não Aplicável	Não Aplicável
		MS26	Proteção de Virtual Private Network (VPN)	X	X	X	X	X	X
		MS27	Proteção de Voice over Internet Protocol (VOIP)		Se aplicável	Se aplicável		Se aplicável	Se aplicável
		MS28	Proteção de Mobile Communications (GSM)			Se aplicável			Se aplicável

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Grupo de Mecanismos	Nome do Grupo	MS ID	Mecanismo de Segurança	Dispositivos			Aplicações		
				Básico	Melhorado	Superior	Básico	Melhorado	Superior
GM06	Criptografia	MS29	Criptografia para acesso remoto	X	X	X	X	X	X
		MS30	Criptografia para segurança de transmissão		X	X		Não Aplicável	Não Aplicável
		MS31	Criptografia para segurança de dados	X	X	X	X	X	X
		MS32	Vetores de inicialização						
		MS33	Gestão de chaves						
		MS34	Interface de introdução/atualização de chaves.						
		MS35	Algoritmo comercial						
		MS36	Zeroization						
		MS37	Manutenção de Sincronismo simples						
		MS38	Manutenção de Sincronismo por duas funções independentes						
		MS39	Manutenção de Sincronismo por três funções independentes OU duas funções fisicamente independentes						
GM07	Dados	MS40	Minimização de Dados	X	X	X	X	X	X
		MS41	Classificação de Dados	X	X	X	X	X	X
		MS42	Prevenção de Exfiltração de Dados		X	X		X	X
GM08	Sustentação da Segurança	MS43	Separação de Dominios	X	X	X	X	X	X
		MS44	Auto-Proteção	X	X	X	X	X	X
		MS45	Inicialização Segura	X	X	X	X	X	X
		MS46	Proteção de Desvios	X	X	X	X	X	X
		MS47	Armazenamento Segregado	X	X	X	X	X	X
		MS48	Prevenção Comportamental			X			X
		MS49	Recuperação Automática			X			X
		MS50	Sincronização Temporal	X	X	X	X	X	X
		MS51	Sincronização de Configuração			X			X
		MS52	Verificação de Indicadores de Compromisso (IOC)		X	X		X	X
GM09	Segurança Eletrónica	MS53	Eficiência Energética	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS54	Reduzida emissão			X	Não Aplicável	Não Aplicável	Não Aplicável
		MS55	Reduzida Interferencia Eletromagnetica (EMI)				Não Aplicável	Não Aplicável	Não Aplicável
		MS56	Elevada Compatibilidade Eletromagnetica (EMC)				Não Aplicável	Não Aplicável	Não Aplicável

B.2. Níveis de Garantia de Segurança

Os requisitos de garantia de segurança são baseados na profundidade da avaliação, no nível de detalhe da documentação, no nível de proteção e no conhecimento de vulnerabilidades sobre os produtos sujeitos a avaliação. Sendo para cada nível considerados os seguintes requisitos:

– Nível BÁSICO:

- Cumprimento dos requisitos do produto;
- Nível de Proteção superior a 0,75;
- Nível de Confiança equivalente a EAL3 do Common Criteria (CC)**;**
- Ausência vulnerabilidades críticas ou de elevado impacto, passiveis de ser exploradas por atores maliciosos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

– Nível MELHORADO:

- Cumprimento dos requisitos do produto;
- Nível de Proteção superior a 0,85;
- Nível de Confiança equivalente a EAL4 do CC**;**
- Ausência vulnerabilidades críticas ou de elevado/moderado impacto, passiveis de ser exploradas por atores maliciosos.

– Nível SUPERIOR:

- Cumprimento dos requisitos do produto;
- Nível de Proteção superior a 0,95;
- Nível de Confiança equivalente a EAL4+ (com AVA_VAN.5) do CC**;**
- Ausência vulnerabilidades críticas ou de elevado/moderado impacto, passiveis de ser exploradas por atores maliciosos.

B.3. Procedimento de avaliação

O OAV deve:

1- Confirmar que se encontram assegurados os requisitos gerais de admissão.
2- Verificar se os requisitos do produto (mecanismos de segurança) para cada nível de garantia se encontram presentes no produto e se o perfil de proteção permite avaliar o produto com um nível de confiança suficiente.
3- Deve analisar o perfil de proteção (padrão CC), em função das características e funcionalidades do produto (em caso de dúvida esclarecer com o OCC).

O OCC deverá ser informado da realização dos ensaios ou inspeções, reservando-se o direito de se pronunciar na eventual seleção ou recolha de amostras por parte do OAV, de verificar as condições em que estas atividades são efetuadas e os respetivos registos e arquivos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO C – Requisitos para Produtos Criptográficos

O processamento de informação classificada, de qualquer grau, requer a utilização de proteção criptográfica, comprovada através da avaliação de algoritmos, módulos, serviços, aplicações e produtos de acordo com os requisitos definidos pela documentação em referência.

O processamento de informação classificada de grau igual ou superior a SECRETO apenas pode ser feito com recurso a algoritmos não comerciais.

A documentação de referência pode ser consultada por qualquer entidade devidamente credenciada junto do OCC.

Consideram-se produtos criptográficos:

- Geradores de chaves;
- Módulos baseados em hardware de cifra, assinatura digital ou funções resumo criptográficas;
- Módulos baseadas em software de cifra, assinatura digital ou funções resumo criptográfica.

O processo de avaliação e certificação de um produto criptográfico tem por base:

- Avaliação de funcionalidades;
- Avaliação de vulnerabilidades;
- Avaliação do nível de Radiação (TEMPEST), se aplicável;
- Avaliação criptográfica;

C.1. Requisitos do produto

Constituem-se como requisitos para produtos criptográficos comerciais os seguintes:

1. Ter todo o software que contribui para a implementação de mecanismos de segurança ou que assegura funções críticas de segurança, assinado digitalmente tendo por base um certificado com chave pública e garantir a sua verificação;
2. Todo o software deve ser rigorosamente testado e examinado minuciosamente quanto a possíveis *trap doors, trojan horses, time bombs* ou qualquer outro código oculto que possa comprometer a segurança;
3. Devem ser selecionados algoritmos para criptografia, gestão de chave, função resumo criptográfica (hash) e assinatura de acordo com referenciais aceites internacionalmente;
4. Todos os algoritmos criptográficos, mecanismos criptográficos, e randomizadores de hardware e software, devem ser igualmente avaliados;
5. Todos os produtos sujeitos a avaliação devem ser entregues com pelo menos os seguintes documentos:
    a. Descrição do conceito de operação com explicação das características de desenho e do modelo de implementação, utilização e ambiente de operação;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

b. Manual de operação;
c. Manual de manutenção;
d. Relatório de avaliação interno pela organização;
e. Descrição do Algoritmo, incluindo a descrição matemática e um diagrama logico com descrição das variáveis criptográficas, incluindo as diferentes etapas e a informação de temporal de cada etapa;
f. Descrição dos diferentes modos de operação e sua aplicabilidade no produto em avaliação;
g. Descrição do processo de inicialização incluindo a caracterização dos protocolos e das mensagens internas;
h. Relatório de Avaliação TEMPEST (para produtos baseados em hardware) com descrição do plano de testes e o resultado da avaliação;
i. Plano de gestão de chaves e especificações técnicas relacionadas com a gestão e destruição de chaves;
j. Desenhos técnicos de cada módulo com descrição de circuitos e inventário de componentes;
k. Descrição detalhada do módulo de configuração e do seu processo interno;
l. Descrição detalhada do software com especial foco para o fluxo de dados em cada módulo e componente e a sua relação e dependência e outros módulos;

6. Para realização de uma avaliação técnica a organização deve facultar cinco unidades para a realização de testes. Duas unidades devem ser utilizadas para a realização de testes do nível de radiação (TEMPEST) e outras duas para teste de funcionalidades e vulnerabilidade, ficando uma como reserva;
7. Adicionalmente devem ainda ser fornecidos dois conjuntos completos de gestão de chaves, cablagem auxiliar e outros componentes que possam ser necessários substituir durante a realização de testes;
8. A implementação de funções criptográficas deve ter por base a utilização de um sistema operacional avaliado e certificado;
9. Os requisitos de funcionalidade encontram-se seguidamente definidos:

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Grupo de Mecanismos	Nome do Grupo	MS ID	Mecanismo de Segurança	Dispositivo			Aplicação		
				Básico	Melhorado	Superior	Básico	Melhorado	Superior
GM01	Auditoria de Segurança	MS01	Análise da Cadeia de Abastecimento	X	X	X		X	X
		MS02	Análise de Conteúdo		X	X		X	X
		MS03	Análise de Conformidade			X			X
		MS04	Análise de Integridade de dados	X	X	X	X	X	X
		MS05	Análise de Registos	X	X	X	X	X	X
		MS06	Análise de Vulnerabilidades	X	X	X	X	X	X
GM02	Identificação, Autenticação e Autorização de acesso	MS07	Identificação e Autenticação	X	X	X	X	X	X
		MS08	Autorização	X	X	X	X	X	X
		MS09	Certificados digitais		X	X		X	X
		MS10	Assinaturas digitais			X			X
		MS11	Infraestrutura de Chaves Públicas			X			X
GM03	Integridade	MS12	Proteção de Integridade de Hardware	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS13	Proteção da Configuração de Hardware	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS14	Proteção da Configuração de Sistema Operativo	X	X	X	X	X	X
		MS15	Proteção da Configuração de Aplicações	X	X	X	X	X	X
		MS16	Proteção de Bibliotecas de Software/Firmware	X	X	X	X	X	X
		MS17	Proteção de Código		X	X		X	X
		MS18	Proteção de Dados	X	X	X	X	X	X
GM04	Disponibilidade	MS19	Proteção Anti-roubo	X	X	X	X	X	X
		MS20	Falha Segura	X	X	X	X	X	X
		MS21	Operação em ambiente degradado	X	X	X		X	X
		MS22	Proteção contra Denial of Service	X	X	X	X	X	X
		MS23	Proteção contra Malware	X	X	X	X	X	X
GM05	Comunicações	MS24	Proteção de Ethernet	Se aplicável	X	X		X	X
		MS25	Proteção de Wireless	Não Aplicável	Não Aplicável	Não Aplicável	Não Aplicável	Não Aplicável	Não Aplicável
		MS26	Proteção de Virtual Private Network (VPN)	X	X	X	X	X	X
		MS27	Proteção de Voice over Internet Protocol (VOIP)		Se aplicável	Se aplicável		Se aplicável	Se aplicável
		MS28	Proteção de Mobile Communications (GSM)		Se aplicável	Se aplicável		Se aplicável	Se aplicável
GM06	Criptografia	MS29	Criptografia para acesso remoto	X	X	X	X	X	X
		MS30	Criptografia para segurança de transmissão	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS31	Criptografia para segurança de dados	X	X	X	X	X	X
		MS32	Vetores de inicialização		X	X		X	X
		MS33	Gestão de chaves	X	X	X	X	X	X
		MS34	Interface de introdução/atualização de chaves	X	X	X	X	X	X
		MS35	Algoritmo comercial	X	X		X	X	
		MS36	Zeroization	X	X	X	X	X	X
		MS37	Manutenção de Sincronismo simples	X			X		
		MS38	Manutenção de Sincronismo por duas ou mais funções independentes		X			X	
		MS39	Manutenção de Sincronismo por duas ou mais funções fisicamente independentes			X			X
GM07	Dados	MS40	Minimização de Dados	X	X	X	X	X	X
		MS41	Classificação de Dados	X	X	X	X	X	X
		MS42	Prevenção de Exfiltração de Dados		X	X		X	X
GM08	Sustentação da Segurança	MS43	Separação de Dominios	X	X	X	X	X	X
		MS44	Auto-Proteção	X	X	X	X	X	X
		MS45	Inicialização Segura	X	X	X	X	X	X
		MS46	Proteção de Desvios	X	X	X	X	X	X
		MS47	Armazenamento Segregado	X	X	X	X	X	X
		MS48	Prevenção Comportamental		X	X		X	X
		MS49	Recuperação Automática		X	X		X	X
		MS50	Sincronização Temporal	X	X	X	X	X	X
		MS51	Sincronização de Configuração			X			X
		MS52	Verificação de Indicadores de Compromisso (IOC)		X	X		X	X
GM09	Segurança Eletrónica	MS53	Eficiência Energética	X	X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS54	Reduzida emissão		X	X	Não Aplicável	Não Aplicável	Não Aplicável
		MS55	Reduzida Interferencia Eletromagnetica (EMI)			X	Não Aplicável	Não Aplicável	Não Aplicável
		MS56	Elevada Compatibilidade Eletromagnetica (EMC)			X	Não Aplicável	Não Aplicável	Não Aplicável

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

C.2. Níveis de Garantia de Segurança

– Nível BÁSICO:

- Cumprimento dos requisitos do produto e demais orientações;
- Nível de Proteção superior a 0,80;
- Nível de Confiança equivalente a EAL3+ (com AVA_VAN.3) do Common Criteria**;**
- Ausência de conhecimento publico sobre vulnerabilidades com criticidade Critica ou Alta; ou Moderada.

– Nível MELHORADO:

- Cumprimento dos requisitos do produto e demais orientações;
- Nível de Proteção superior a 0,90;
- Nível de Confiança equivalente a EAL4+ (com AVA_VAN.4) do Common Criteria**;**
- Ausência vulnerabilidades de conhecimento público.

– Nível SUPERIOR:

- Cumprimento dos requisitos do produto e demais orientações;
- Nível de Proteção superior a 0,95;
- Nível de Confiança equivalente a EAL5+ (com AVA_VAN.5) do Common Criteria**;**
- Ausência vulnerabilidades de conhecimento público.

C.3. Requisitos do Relatório de Avaliação Técnica:

O relatório deve seguir o modelo definido no anexo L do presente Esquema, com as necessárias adaptações, devendo ainda conter:

- Descrição do processo de programação/codificação;
- Descrição do processo de produção;
- Descrição do sistema de gestão;
- Descrição da cadeia de abastecimento;
- Descrição dos níveis de impacto e dependência aferidos para a cadeia de abastecimento;
- Descrição dos procedimentos de operação em segurança;
- Plano de atividades de acompanhamento do produto.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

C.4. Orientação sobre criptografia implementada em hardware configurável ou reconfigurável uma só vez

Os bits de configuração que determinam a configuração das funções de segurança em hardware configurável devem ser desenvolvidos com segregação de ambientes de produção e de teste.

Cada vez que um algoritmo ou curva elíptica é carregada a partir da memória, deve ser realizada uma verificação da integridade sobre toda a informação carregada.

A função carregada deve ser testada para aferir se está a funcionar conforme previsto.

O processo de reconfiguração de hardware deve ser testado, autenticado, verificada a sua integridade e assinado digitalmente.

A função que verifica a assinatura digital deve ser implementada em hardware confiável não reconfigurável.

Para o nível de garantia Superior, a deteção de erros em tempo real para funções de segurança implementadas em hardware reconfigurável (ou configurável uma vez) deve comparar as saídas de pelo menos dois dispositivos de hardware fisicamente independentes em vez de saídas de diferentes áreas de um único dispositivo.

Para o nível de garantia Superior, um produto criptográfico que implemente algoritmos criptográficos e outras funções de segurança em hardware que não seja um ASIC, ou uma FPGA, deve ter pelo menos dois dispositivos de hardware fisicamente independentes nos quais são implementadas funções independentes.

Para o nível de garantia Melhorado, a deteção de erros em tempo real para funções de segurança implementadas em hardware reconfigurável (ou configurável uma vez) pode comparar as saídas de apenas um único dispositivo de hardware fisicamente independentes.

Para o nível de garantia Melhorado, um produto criptográfico que implemente algoritmos criptográficos e outras funções de segurança em hardware que não seja um ASIC, ou uma FPGA, deve ter pelo menos uma função independente.

Produtos que usam hardware reconfigurável ou hardware com circuitos não utilizados disponíveis, devem possuir mecanismos que permitam detetar adulterações por diferentes meios.

C.5. Orientação sobre criptografia implementada através de uma aplicação de software

O software que implementa funções de segurança através de uma aplicação deve ser desenvolvido usando um processo de desenvolvimento estruturado.

Todas as funções de segurança implementadas através de uma aplicação devem ser testadas com testes positivos e negativos.

Antes da instalação, todas as aplicações que implementam criptografia devem ser autenticadas usando uma assinatura digital.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

As chaves usadas para proteger criptograficamente o tráfego, designadas por Chave de Criptografia de Tráfego (TEK), devem permanecer criptografadas quando em uso ou quando carregadas em memória volátil.

A Chave de Criptografia de Chave (KEK) deve ser protegida assegurando que a mesma, ou uma parte dela, resida fora do dispositivo ou estação de trabalho.

Para manter a garantia de que a criptografia implementada no software de aplicação continua a funcionar corretamente, todas as funções de segurança devem ser testadas periodicamente.

C.6. Orientações sobre gestão de chaves

Os mecanismos de confidencialidade e integridade devem ter chaves e certificados separados de outros mecanismos criptográficos. Em particular, o uso do mesmo par de chaves assimétricas para mais de uma finalidade deve ser evitado.

O material respeitante à chave privada ou material de inicialização secreto deve ser distribuído de forma segura, por exemplo através de um *token* fisicamente seguro ou protegido por um mecanismo de segurança.

O material de inicialização de chaves secreto deve ser armazenado junto do produto num token fisicamente seguro ou num ambiente seguro.

A recuperação ou arquivamento de parte da chave privada dos Esquemas de assinatura digital utilizados para serviços de não repúdio não deve ser possível.

Os certificados de chave pública usados para serviços de não repúdio precisam ser arquivados por um período adequado para posterior verificação dos objetos assinados.

Se as chaves forem carregadas, deve haver uma interface dedicada para o carregamento de chaves por forma a reforçar o isolamento da chave.

C.7. Orientação sobre criptografia simétrica

A segurança oferecida por chaves simétricas deve ser, no mínimo, de 256 bits.

O mecanismo de criptografia deve ser usado em conjunto com um mecanismo de integridade, devendo estes ser independentes um do outro, no mínimo, em termos dos segredos de cifra e de integridade.

Os métodos de integridade simétrica devem ser baseados em cifras de bloco ou mecanismos de *hash,* em que o nível de força de tais primitivas deve estar de acordo com o nível de garantia necessário para o mecanismo resultante.

A escolha do algoritmo simétrico deve determinar a escolha do modo de *key wrap* que, por conseguinte, determina o modo de escolha de atualização da chave.

O modo *key wrap* deve ser usado quando as chaves criptográficas são distribuídas através de canais não seguros ou quando são armazenadas para tratamento de dados em repouso.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

O modo de escolha de atualização da chave pode ser usado para substituir uma chave existente por uma nova, desde que relacionadas.

C.8. Orientação sobre criptografia assimétrica

Não devem ser utilizados mecanismos criptográficos de chave pública baseados no problema clássico do Logaritmo Discreto.

O nível de garantia Superior só deve utilizar mecanismos criptográficos baseados em curvas elípticas definidas sobre GF(p).

Desaconselha-se a utilização do algoritmo RSA, não obstante, se for utilizado, deve-se utilizar o tamanho mínimo do módulo igual a 4096 bits.

Para o nível de garantia Melhorado e Superior, o tamanho mínimo do módulo deve ser de 4096 bits, devendo o expoente público (p) e expoente privado (q), ser primos, gerados aleatoriamente e ter um valor superior a (2^{255}+1).

Uma Curva Elíptica deve possuir parâmetros de 256bits ou 384 conforme se trate do nível de garantia Padrão ou do nível de garantia Melhorado ou Superior.

C.9. Orientação sobre funções de Hash

Para todos os níveis de garantia, o tamanho mínimo de *hash* gerado por uma função de *hash* deve ser de 384 bits. Além disso, quando usado para assinatura digital em combinação com curvas elípticas, o tamanho da saída da função *hash* deve ser semelhante (da mesma ordem) ao comprimento de bits da curva elíptica subjacente.

Para todos os níveis de garantia, nenhum ataque, mesmo parcial, deve ser conhecido, exceto os ataques genéricos.

C.10. Orientação sobre geração de números aleatórios

Para todos os níveis de garantia, pode ser utilizado um gerador de números aleatórios devidamente avaliado, certificado e aprovado.

O *randomizador* e todas as primitivas criptográficas usadas com ele devem possuir o mesmo nível de garantia de segurança.

O *randomizador* deve possuir nível de garantia de segurança associado à quantidade de trabalho (ou seja, o número de operações) necessário para quebrar um algoritmo ou sistema criptográfico.

O nível de garantia de segurança é especificado em bits e é um valor específico do conjunto {192, 256,384, 512}.

Se o nível de garantia de segurança associada a um algoritmo ou sistema determinístico for X bits, espera-se que sejam necessárias 2^X operações básicas (aproximadamente) para quebrá-lo.9

[9] Tradução livre de NIST Special Publication 800-90A Revision 1.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

O nível de entropia calculado para os outputs de um gerador, em baixo representada pela equação de Shannon, em baixo apresentada, não deve ser inferior a 0,9.[10]

$$H(X) = -\sum x \in S \cdot px \cdot log2(px)$$

C.11. Orientação sobre algoritmos

Para todos os níveis de garantia, apenas devem ser usados algoritmos abaixo indicados:

Serviço Cifra	Tipo A	Tipo B	Parâmetro
Encriptação Simétrica	Trebaruna	AES-256	256
Estabelecimento de Chaves	EC-DH	EC-DH	384
Hash	SHA-2 HMAC	SHA-2/SHA-3	384
Assinatura Digital	EC-DSA	EC-DSA	384
	-	RSA (em fim de vida)	4096

C.12. Orientação sobre TLS

Para todos os níveis de garantia, apenas devem ser usados *chipher suites* abaixo indicados:

TLS 1.3

- TLS_AES_256_GCM_SHA384
- TLS_AES_256_GCM_SHA256
- TLS_AES_256_CCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

[10] Calculado conforme definido pela norma ISO/IEC 20543:2019(en) Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

C.13. Algoritmos criptográficos não comerciais

A ANS é responsável por desenvolver, avaliar e certificar os algoritmos criptográficos nacionais utilizados para o processamento de informação classificada.

C.14. Procedimentos de avaliação

O OAV deve:

1- Confirmar que se encontram assegurados os requisitos gerais de admissão;
2- Verificar se os requisitos do produto (mecanismos de segurança) para cada nível de garantia se encontram presentes no produto e se o Perfil de Proteção permite avaliar o produto com um nível de confiança adequado;
3- Analisar o perfil de proteção em função das suas características e funcionalidades.

O OCC deverá ser informado da realização dos ensaios ou inspeções, reservando-se o direito de se pronunciar na eventual seleção ou recolha de amostras por parte do OAV, de verificar as condições em que estas atividades são efetuadas, os respetivos registos e arquivos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO D – Requisitos para Produtos Baixa Radiação (TEMPEST)

D.1. Requisitos do produto

Os produtos utilizados para o processamento de informação classificada (equipamentos, acessórios, cabos, etc.), de grau igual ou superior a NACIONAL CONFIDENCIAL, requerem a utilização de equipamentos com um baixo nível de radiação, comprovado através da avaliação da radiação de acordo com os requisitos definidos pelo GNS.

A avaliação de produtos de baixa radiação (TEMPEST) é feita em Laboratório acreditado pelo IPAC, devendo para mais informação ser contactados os Laboratórios aprovados.

A documentação de referência pode ainda ser consultada por qualquer entidade devidamente credenciada junto do OCC.

Os testes de radiação devem observar os seguintes princípios:

- No caso de computadores, estações de trabalho ou produtos TIC comparáveis, os produtos são testados em termos de emissões e aprovados como um sistema informático com uma configuração correspondente a um dispositivo básico, um teclado, um monitor, e se necessário um rato;
- O estado do dispositivo de todos os componentes testados em termos de emissões, incluindo cablagem, é registado e documentado;
- A documentação do teste deve demonstrar como os diferentes componentes se relacionam (o dispositivo, o monitor, o teclado e se necessário, também o rato). A entrega deve ocorrer de forma que o destinatário possa reconhecer diretamente esse conjunto de dispositivos relacionados;
- Somente produtos listados individualmente (por exemplo, impressora ou scanner) são passiveis de ser aferidos individualmente;
- Se um sistema informático protegido contra radiação for construído a partir de componentes que já foram aprovados noutros processos, é criado um produto com um nome de produto diferente, que deve ser submetido a avaliação;
- A substituição de componentes individuais só é permitida se forem utilizados componentes avaliados e listados para o mesmo dispositivo;
- Se um destes componentes for alterado e o status do dispositivo for alterado, trata-se de um novo produto sem certificação;
- Se for adicionado um ou mais componentes (por ex. expandir um sistema de computador para incluir um monitor ou placa de rede adicional), resultará na perda de certificação;
- Componentes e cabos que não foram testados quanto à radiação **não podem** ser incluídos no pacote;
- Uma lista de componentes do dispositivo testado, incluindo a cablagem, deve sempre ser anexada ao relatório de avaliação do produto;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- Dispositivos que apresentam defeitos visíveis ou reconhecíveis, como parafusos soltos, vedações ou partes soltas, ferrite ou juntas de proteção com folga ou livres, devem ser rejeitados e o OCC informado.

D.2. Níveis de Garantia de Segurança:

O desenvolvimento de produtos de baixa radiação (TEMPEST) possui um conjunto adicional de documentação e requisitos que podem ser consultados junto do OCC.

A avaliação dos requisitos funcionais deve ser feita com base no modelo de teste aprovado por um laboratório aprovado, não sendo aplicado a serviços.

– Nível BÁSICO:

- Cumprimento dos requisitos do produto;
- Equipamento avaliado com nível C de acordo com o documento SDIP27/2, ou Equipamento Zona 2 do Modelo de Zona.

– Nível MELHORADO:

- Cumprimento dos requisitos do produto;
- Equipamento avaliado como nível B de acordo com o documento SDIP27/2 ou Equipamento Zona 1 do Modelo de Zona.

– Nível SUPERIOR:

- Cumprimento dos requisitos do produto;
- Equipamento avaliado como nível A de acordo com o documento SDIP27/2, ou Equipamento Zona 0 do Modelo de Zona.

D.3. Requisitos do Relatório de Avaliação Técnica

O relatório deve seguir o modelo definido no anexo L, com as necessárias adaptações por forma a se constituir como um modelo laboratorial pré-determinado.

D.4. Procedimentos

O OAV após verificar que se encontram assegurados os requisitos gerais de admissão ao presente Esquema, deve analisar as características e ergonomia do produto por forma a ser inserido em câmara anecoica e avaliado.

O OAV pode endereçar ao OCC quaisquer dúvidas ou propostas de avaliação, dispondo o último de 15 dias úteis para se pronunciar sobre as referidas dúvidas e exequibilidade da proposta de avaliação.

O OCC reserva ainda o direito de estar presente durante a realização dos ensaios ou inspeções, na eventual seleção ou recolha de amostras por parte do OAV, verificar as condições em que estas atividades são efetuadas, os respetivos registos e arquivos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO E – Requisitos para Serviços de Computação em Nuvem

E.1. Requisitos do serviço

O Serviço de Computação em Nuvem pode assumir diferentes topologias, designadamente:

- *IAAS – Infrastructure as a Service*
- *PAAS – Platform as a Service*
- *SAAS – Software as a Service*
- *3rd Party – 3rd Party Application as a Service*

Constituem-se como requisitos do serviço (mecanismos de segurança) a observar:

Requisitos de segurança da informação para plataformas de nuvem GNS_V3.0					
		PROVEDOR			3th Party APP
CLASSE	TIPO	IAAS	PAAS	SAAS	
Application & Interface Security	Teste/Documentação	X	X	X	X
Identity and Access Management	Teste/Documentação	X	X	X	X
Business Continuity Management and Operational Resilience	Documentação	X	X		
Security Governance and Risk Management	Documentação	X	X	X	
Infrastructure and Virtualization Security	Teste/Documentação	X	X		
Interoperability and Portability	Teste/Documentação	X	X		
Mobile Security	Teste/Documentação		X	X	X
Security Incident Management, e-Discovery and Cloud Forensics	Documentação	X	X	X	X
Logging & Monitoring	Teste/Documentação	X	X	X	X
Threats and Vulnerabilities Management	Teste/Documentação	X	X	X	X
Endpoint Security	Teste/Documentação	X	X	X	
User Documentation	Documentação	X	X	X	X
Data Security and Information Management	Documentação	X	X	X	X
Encryption and Key Management	Teste/Documentação	X	X	X	X
Change Control and Configuration Management	Documentação	X	X	X	X
Supply Chain Security	Documentação	X	X		
Awareness and Training	Documentação	X	X	X	
Audit Assurance and Compliance	Teste/Documentação	X	X	X	X
Organization of Information Security	Documentação	X	X	X	
Legal Process	Documentação	X	X		
Global / Local / Electronic Security Environment	Inspeção Física/ Documentação	X	X		
Personnel Security	Inspeção Física/ Documentação	X	X	X	

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

A avaliação de *3rd Party Application as a Service* poderá ainda ser sujeita a outras avaliações no âmbito de produtos comerciais não criptográficos incidentes sobre a respetiva aplicação de software.

E.2. Níveis de Garantia de Segurança

Os serviços de computação em nuvem apenas se encontram autorizados a processar informação classificada de acordo com os requisitos de garantia de segurança **BÁSICO**, compreendendo:

- Cumprimento de todos os controlos constantes nos requisitos do serviço;
- Nível de Confiança equivalente a EAL3 do Common Criteria (apenas para *3rd Party Application as a Service)***;**
- Ausência de conhecimento publico sobre vulnerabilidades com criticidade Critica ou Alta.

E.3. Requisitos do Relatório de Avaliação Técnica

O relatório deve seguir o modelo definido no anexo L do presente Esquema, com as necessárias adaptações, devendo ainda conter:

- Descrição das principais questões para acesso à plataforma, incluindo a cadeia de abastecimento;
- Descrição da configuração mínima de segurança a adotar.

E.4. Procedimento de avaliação

O OAV deve:

1- Verificar que se encontram assegurados os requisitos gerais de admissão;
2- Verificar se os requisitos do serviço (mecanismos de segurança) para cada nível de garantia se encontram presentes no produto e se o Perfil de Proteção permite avaliar o produto com um nível de confiança adequado;
3- Deve analisar o perfil de proteção em função das suas características e funcionalidades.

O OCC reserva o direito de estar presente durante a realização dos ensaios ou inspeções, na eventual seleção ou recolha de amostras por parte do OAV, verificar as condições em que estas atividades são efetuadas, os respetivos registos e arquivos.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO F – Descrição dos Mecanismos de segurança

Grupo de Mecanismos	Nome do Grupo	MS ID	Mecanismo de Segurança	Descrição do Mecanismo de Segurança
GM01	Auditoria de Segurança	MS01	Análise da Cadeia de Abastecimento	Mecanismos de segurança que visem assegurar a confiança na cadeia de abastecimento, no que diz respeito a dependêncais tecnologicas e alterações inseridas no firmware, onde se inclui o Trusted Plataform Module (TPM).
		MS02	Análise de Conteúdo	Mecanismos de segurança que visem assegurar o conteúdo de mensagens e protocolos, designadamente através da constituição de Proxys/Reverse Proxys ou outros processos.
		MS03	Análise de Conformidade	Mecanismos de segurança que visem assegurar a manutenção da conformidade de produtos ou serviços em relação a uma base segura de comparação aprovada.
		MS04	Análise de Integridade de dados	Mecanismos de segurança que visem assegurar a integridade dos dados quer através de cyclic redundancy check (CRC) ou outro processo semelhante.
		MS05	Análise de Registos	Mecanismos de segurança que visem assegurar a existência, manutenção e fiabilidade nos registos internos de produtos ou serviços.
		MS06	Análise de Vulnerabilidades	Mecanismos de segurança que visem assegurar um a avaliação de vulnerabilidades em produtos ou serviços durante a sua utilização.
GM02	Identificação, Autenticação e Autorização de acesso	MS07	Identificação e Autenticação	Mecanismos de segurança que visem assegurar a correcta identificação e autenticação de utilizadores de produtos ou serviços, incluindo a utilização de multiplos fatores de identificação e autenticação.
		MS08	Autorização	Mecanismos de segurança que visem assegurar a correta autorização a utilizadores de produtos ou serviços para manipular dispositivos ou dados, incluindo os processos de gestão de privilégios e de mudança de um utilizador para outro utilizador.
		MS09	Certificados digitais	Mecanismos de segurança que visem assegurar a confiança na utilização de certificados digitais em produtos ou serviços, designadamente para autenticação de produtos ou serviços e identificação de utilizadores.
		MS10	Assinaturas digitais	Mecanismos de segurança que visem assegurar a confiança na utilização de assinaturas digitais em produtos ou serviços, designadamente para identificação e autenticação de utilizadores e reconhecimento de produtos.
		MS11	Infraestrutura de Chaves Públicas	Mecanismos de segurança que visem assegurar a confiança na utilização de uma Infraestrutura de Chave Públicas em produtos ou serviços.
GM03	Integridade	MS12	Proteção de Integridade de Hardware	Mecanismos de segurança que visem assegurar a proteção da integridade do hardware, no que diz respeito a poder ser alterado após o arranque. Incluem-se aqui os mecanismos de arranque seguro.
		MS13	Proteção da Configuração de Hardware	Mecanismos de segurança que visem assegurar a proteção da configuração do hardware contra alterações não controladas do mesmo.
		MS14	Proteção da Configuração de Sistema Operativo	Mecanismos de segurança que visem assegurar a proteção da configuração de sistemas operativos contra alterações acidentais ou intencionais dos não autorizadas do mesmo.
		MS15	Proteção da Configuração de Aplicações	Mecanismos de segurança que visem assegurar a proteção da configuração de aplicações contra alterações acidentais ou intencionais mas não autorizadas das mesmas.
		MS16	Proteção de Bibliotecas de Software/Firmware	Mecanismos de segurança que visem assegurar a proteção de bibliotecas de softwarecontra alterações acidentais ou intencionais mas não autorizadas das mesmas. Inclui proteções básicas (Canary, NX, PIE, RELRO) e avançadas (Fortify, CFI, SafeStack, ASLR) entre outras.
		MS17	Proteção de Código	Mecanismos de segurança que visem assegurar a proteção do código contra alterações acidentais ou intencionais mas não autorizadas do mesmo.
		MS18	Proteção de Dados	Mecanismos de segurança que visem assegurar a proteção dos dados, através de software, contra o mau uso e a realização de alterações acidentais ou intencionais não autorizadas dos mesmos. Este mecanismo visa garantir a disponibilidade dos dados, excluindo-se a confidencialidade e a integridade.
GM04	Disponibilidade	MS19	Proteção Anti-roubo	Mecanismos de segurança que visem assegurar a proteção do hardware contra roubo ou desvio. Incluem-se neste grupo os mecanismos de geo-localização, entre outros.
		MS20	Falha Segura	Mecanismos de segurança que visem assegurar a proteção de falhas não controladas do hardware.
		MS21	Operação em ambiente degradado	Mecanismos de segurança que visem assegurar a operação de um produto com segurança ainda que num ambiente limitado/degradado.
		MS22	Proteção contra Denial of Service	Mecanismos de segurança que visem assegurar a proteção contra processo que visem a dipsonibilidade de um produto.
		MS23	Proteção contra Malware	Mecanismos de segurança que visem assegurar a proteção de produtos ou serviços contra a propagação de malware nas suas diferentes formas. Incluem-se aqui os vários produtos Anti-virus.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Grupo de Mecanismos	Nome do Grupo	MS ID	Mecanismo de Segurança	Descrição do Mecanismo de Segurança
GM05	Communicações	MS24	Proteção de Ethernet	Mecanismos de segurança que visem proteger uma rede ethernet, contra o mau uso e a proliferação de alterações acidentais ou intencionais mas não autorizadas das mesmas.
		MS25	Proteção de Wireless	Mecanismos de segurança que visem proteger uma rede wireless, contra o mau uso e a proliferação de alterações acidentais ou intencionais mas não autorizadas das mesmas.
		MS26	Proteção de Virtual Private Network (VPN)	Mecanismos de segurança que visem proteger a utilização de uma VPN, contra o mau uso e a proliferação de alterações acidentais ou intencionais mas não autorizadas das mesmas.
		MS27	Proteção de Voice over Internet Protocol (VOIP)	Mecanismos de segurança que visem proteger a utilização de produtos ou serviços VOIP, contra o mau uso e a proliferação de alterações acidentais ou intencionais mas não autorizadas das mesmas.
		MS28	Proteção de Mobile Communications (GSM)	Mecanismos de segurança que visem proteger uma rede GSM, contra o mau uso e a proliferação de alterações acidentais ou intencionais mas não autorizadas das mesmas.
GM06	Criptografia	MS29	Criptografia para acesso remoto	Mecanismos de segurança que visem assegurar a confidencialidade dos dados em processamento e em trânsito. Incluem-se aqui mecanismos relacionados com SSL/TLS, SSH.
		MS30	Criptografia para segurança de transmissão	Mecanismos de segurança que visem assegurar a confidencialidade dos dados em trânsito. Incluem-se aqui mecanismos relacionados com IPSEC, GRE, etc.
		MS31	Criptografia para segurança de dados	Mecanismos de segurança que visem assegurar a confidencialidade dos dados em repouso. Incluem-se aqui mecanismos relacionados com a utilização de produtos de file encryption e drive encryption.
		MS32	Vetores de inicialização	Mecanismos de segurança que visem assegurar a confiança nos vetores de inicalização.
		MS33	Gestão de chaves	Mecanismos de segurança que visem assegurar a confiança no processod e gestão de chaves criptográficas.
		MS34	Interface de introdução/atualização de chaves	Mecanismos de segurança que visem assegurar a confiança no interface de atualização de chaves criptográficas.
		MS35	Algoritmo comercial	Mecanismos de segurança que assegurarem a confiança na utilização de algoritmos criptográficos comerciais.
		MS36	Zeroization	Mecanismos de segurança que visem assegurar a destruição de chaves em caso de emergência.
		MS37	Manutenção de Sincronismo simples	Mecanismos de segurança que visem assegurar a manutenção do sincronismo *keep alive* do produto criptografico.
		MS38	Manutenção de Sincronismo por duas ou mais funções independentes	Mecanismos de segurança que visem assegurar a manutenção do sincronismo *keep alive* do produto criptografico por duas funções independentes.
		MS39	Manutenção de Sincronismo por duas ou mais funções fisicamente independentes	Mecanismos de segurança que visem assegurar a manutenção do sincronismo *keep alive* do produto criptografico por funções fisicamente independentes.
GM07	Dados	MS40	Minimização de Dados	Mecanismos de segurança que visem assegurar que os produtos apenas processam os dados, pessoais ou outros, que sejam adequados, relevantes e limitados ao necessário em relação ao uso pretendido para o produto, assim como, apenas os conservam apenas durante o tempo necessário para cumprir uma dada finalidade.
		MS41	Classificação de Dados	Mecanismos de segurança que visem assegurar a classificação de dados, no que diz respeito a sua utilização, privacidade ou segurança.
		MS42	Prevenção de Exfiltração de Dados	Mecanismos de segurança que visem prevenir a exfiltração de dados de forma acidental ou intencionalmente sem autorização.
GM08	Sustentação da Segurança	MS43	Separação de Dominios	Mecanismos de segurança que visem assegurar a separação fisica ou lógica de dominios ou que reforcem a definição de politicas que reforcem esta separação.
		MS44	Auto-Proteção	Mecanismos de segurança que visem assegurar a auto-proteção da plataforma utilizada para o processamento de dados.
		MS45	Inicialização Segura	Mecanismos de segurança que visem assegurar uma inicialização segura da plataforma utilizada para o processamento de dados.
		MS46	Proteção de Desvios	Mecanismos de segurança que visem assegurar que os mecanismos de segurança não podem ser contornados por outros processos.
		MS47	Armazenamento Segregado	Mecanismos de segurança que visem assegurar a segregação logica do armazenamento de dados num produto ou serviço. Incluem-se aqui a utilização de Trusted Execution Enviroment (TEE).
		MS48	Prevenção Comportamental	Mecanismos de segurança que visem prevenir a existência de comportamentos que coloquem em risco a segurança de dados ou informação em produtos ou serviços.
		MS49	Recuperação Automática	Mecanismos de segurança que visem assegurar a recuperação automatica de um produto ou serviço, para um estado seguro e pré-configurado.
		MS50	Sincronização Temporal	Mecanismos de segurança que visem prevenir a perda de sincronização temporal de produtos ou serviços.
		MS51	Sincronização de Configuração	Mecanismos de segurança que visem prevenir a perda de sincronização de produtos ou serviços com uma configuração remota devidamente aprovada e mantida por uma entidade.
		MS52	Verificação de Indicadores de Compromisso (IOC)	Mecanismos de segurança que visem assegurar a verificação da existência de indicadores de compromisso (IOC) em produtos ou serviços antes da sua utilização normal.
GM09	Segurança Eletrónica	MS53	Eficiência Energética	Mecanismos de segurança que visem assegurar a eficiente utilização da energia usados pelo produtos.
		MS54	Reduzida Emissão	Mecanismos de segurança que visem assegurar uma reduzida emissão de frequências em produtos que utilizem o espectro eletromagnetico.
		MS55	Reduzida Interferencia Eletromagnetica (EMI)	Mecanismos de segurança que visem assegurar uma reduzida interferência eletromagnetica em produtos que utilizem o espectro eletromagnetico.
		MS56	Elevada Compatibilidade Eletromagnetica (EMC)	Mecanismos de segurança que visem assegurar uma elevada compatibilidade eletromagnetica em produtos que utilizem o espectro eletromagnetico.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO G – Requisitos mínimos de segurança para ambientes de desenvolvimento de produtos de nível Melhorado e Superior

As entidades que pretendem desenvolver produtos de nível Melhorado ou Superior, devem possuir ambientes de desenvolvimento devidamente habilitados no âmbito da segurança da informação.

Constituem-se como requisitos de habilitação para as EReq que realizem atividades de desenvolvimento de produtos de nível Melhorado e Superior os seguintes:

G.1. Administração e Organização de Segurança

- A EReq deve definir a estrutura jurídica e organizacional responsável pela confidencialidade e integridade do TOE.
- A EReq deve estabelecer uma estrutura de segurança que apoie o estabelecimento, implementação, operação, monitorização, revisão, manutenção e melhoria de uma Política de Segurança da Informação (PSI), designando pelo menos uma ou mais pessoas para a função de Encarregado de Segurança e fornecendo os recursos necessários.
- A EReq deve nomear pelo menos um Encarregado de Segurança para o ambiente de desenvolvimento, produção e teste do TOE.
- O(s) Encarregado(s) de Segurança deve(m) ser responsável(is) pela segurança geral do ambiente de desenvolvimento, produção e teste do TOE e durante todo o ciclo de vida deste, incluindo a gestão de subcontratados que possam ser usados em algumas atividades. Nesta função, o Encarregado de Segurança do TOE deve reportar diretamente à Administração da EReq.
- Todas as funções e responsabilidades organizacionais devem estar bem definidas e documentadas, existindo pelo menos fluxos de trabalho, descrições de funções, competências necessárias e organograma.
- Quando aplicável, devem existir medidas organizacionais que garantam a segregação de funções entre desenvolvimento, produção, testes, garantia de qualidade e segurança.

G.2. Sistemas de Gestão da Segurança da Informação

- A EReq deve possuir um Sistema de Gestão de Segurança da Informação que salvaguarde a informação comercial, a propriedade intelectual e a privacidade.
- O Sistema de Gestão de Segurança da Informação deve ser implementado de acordo com a norma ISO 27001.
- O Sistema de Gestão de Segurança da Informação deve ser certificado por um organismo de certificação acreditado pelo IPAC para tal certificação.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

G.3. Instruções de Segurança do Projeto (ISP)

- Para além da Política de Segurança da Organização, a EReq deverá possuir uma Política de Segurança especifica para o projeto em causa, ao qual se designa por Instruções de Segurança do Projeto (ISP).
- A ISP deverá ser aprovada pela ANS.
- A ISP deve ser adequada e descrever as medidas físicas, lógicas, procedimentais, de pessoal e outras medidas de segurança que são necessárias para proteger a confidencialidade e integridade do projeto do TOE e sua implementação no ambiente de desenvolvimento, produção e testes.
- A ISP e documentação anexa deve dar conta de todos os locais onde ocorre o desenvolvimento, as atividades de desenvolvimento e as medidas de segurança aplicadas a cada local, assim como, as medidas de segurança especificas para transportes entre diferentes locais.
- A ISP deve, dentro do contexto das atividades comerciais gerais da EReq e dos riscos que a mesma enfrenta, prever como a organização deve estabelecer, implementar, operar, monitorar, manter, rever e melhorar a documentação existente.
- A ISP deve definir uma abordagem de avaliação de risco da EReq, incluindo uma metodologia de avaliação de risco adequada às necessidades de segurança identificadas e cumprimento das obrigações legais e regulamentares para proteger o TOE, incluindo:
    - formular um plano de tratamento de risco que identifique a ação de gestão apropriada, recursos, responsabilidades e prioridades para gerir riscos de segurança;
    - implementar o plano de tratamento de riscos para atingir os objetivos de controlo identificados, o que inclui a consideração do financiamento e a atribuição de funções e responsabilidades;
    - descrever todos os objetivos e controlos selecionados e sua implementação, incluindo os processos e procedimentos operacionais necessários.
- As ameaças tratadas por medidas de segurança apropriadas devem incluir:
    - "Ameaça acidental": possibilidade de erro ou omissão humana, não intencional, mau funcionamento de equipamento ou desastre natural;
    - Ameaça intencional": possibilidade de ataque por uma outra entidade (por exemplo, um hacker individual ou uma organização criminosa). Exemplos de tais ataques são roubo ou furto, troca intencional do TOE ou de suas partes e clonagem.
- A ISP deve ainda incluir:
    - declarações documentadas da política e dos seus objetivos;
    - o âmbito da ISP;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

  - uma descrição da organização e das funções relevantes;
  - procedimentos organizacionais documentados considerados necessários para garantir o planeamento, operação e controlo eficaz dos processos de segurança;
  - um quadro para a definição de objetivos e estabelecer um sentido geral de direção e princípios de ação no que diz respeito às necessidades de integridade e confidencialidade do TOE.
- A ISP documentará as políticas de confidencialidade e integridade do desenvolvimento que detalham:
  - as informações relacionadas com o desenvolvimento do TOE que precisam ser mantidas confidenciais e quais os membros da equipa que têm permissão para aceder a essas informações;
  - o material que deve ser protegido contra modificações não autorizadas, para preservar a integridade do TOE, e quais membros da equipa autorizados a modificar tal material.
- A ISP deverá assinalar a necessidade de estabelecer acordos de confidencialidade ou de não divulgação que reflitam as necessidades de proteção de informação, dados e materiais, devendo ainda estabelecer o seu processo de revisão.
- Os documentos exigidos pela ISP devem ser controlados e protegidos, devendo existir um procedimento documentado para definir as ações de gestão necessárias para:
  - aprovar documentos quanto à sua adequação antes da emissão;
  - rever e atualizar documentos conforme necessário, assim como, a reaprovação;
  - garantir que as alterações e o estado atual de revisão dos documentos sejam identificados;
  - garantir que os documentos permaneçam legíveis e facilmente identificáveis;
  - garantir que os documentos estejam disponíveis para quem deles necessita e sejam transferidos, armazenados e, em última instância, eliminados de acordo com os procedimentos aplicáveis à sua classificação;
  - evitar a utilização não intencional de documentos obsoletos;
  - aplicar-lhes uma identificação e classificação adequada caso sejam retidos para qualquer finalidade.
- Para garantir que a ISP esteja atualizada, a EReq deve, regularmente:
  - realizar revisões regulares da eficácia da ISP, tendo em conta os resultados das auditorias de segurança, incidentes, sugestões e feedback de todas as partes interessadas;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

  - rever as avaliações de risco em intervalos planeados em particular os riscos residuais e os níveis aceitáveis de riscos identificados;
  - realizar auditorias internas em intervalos planeados conforme definido na ISP;
  - implementar as melhorias identificadas;
  - tomar ações corretivas e preventivas apropriadas;
  - aplicar as lições aprendidas com as experiências de segurança de outras organizações e da própria organização;
  - comunicar as ações e melhorias a todas as partes interessadas com um nível de detalhe adequado às circunstâncias;
- Os registos devem ser criados e mantidos para fornecer evidências de conformidade com os requisitos, incluindo a operação eficaz da ISP. Devem ainda ser adequadamente protegidos e controlados, permanecer legíveis, facilmente identificáveis e recuperáveis. Os controlos necessários para a sua identificação, armazenamento, proteção, recuperação, tempo de retenção e disposição de registos devem ser documentados e implementados.
- Devem ser mantidos registos da operação dos processos e de todas as ocorrências de incidentes de segurança significativos relacionados com o TOE.

G.4. Acreditação no âmbito da segurança da informação classificada

- A EReq deve estar devidamente credenciada e possuir um posto de controlo;
- A EReq deve garantir que o ambiente de desenvolvimento é devidamente acreditado do ponto de vista da segurança da informação classificada pela ANS, na marca e grau requerido.
- A acreditação de segurança da informação classificada de qualquer ambiente segue as regras da acreditação de sistemas de informação e de comunicação (SIC) em vigor para sistemas que processam informação classificada, aprovadas pelo GNS.
- Cada ambiente deve implementar os requisitos de segurança necessários para o grau de classificação requerido.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO H – Modelo de Acordo de Confidencialidade

ACORDO DE REGULAÇÃO DA CONFIDENCIALIDADE E DA PROPRIEDADE INTELECTUAL RESULTANTE DO PROCESSO DE AVALIAÇÃO E CERTIFICAÇÃO

Entre:

Gabinete Nacional de Segurança (GNS), com sede na Rua da Junqueira, 69, 1300-342, em Lisboa, Pessoa Coletiva n.º 600 056 120, representada por _____, na qualidade de Organismo de Certificação da Conformidade, com poderes legais e estatutários de representação, como Primeiro Outorgante, doravante designado GNS.

e

[NOME EMPRESA], com sede na [MORADA], Pessoa Coletiva nº [NÚMERO], representada por [NOME], na qualidade de Entidade Responsável pelo produto/serviço [NOME DO PRODUTO/SERVIÇO], com poderes legais de representação, como Segundo Outorgante, doravante designada por EMPRESA.

Adiante designados, em conjunto, por outorgantes ou partes,

Considerando:

a) Que o GNS desenvolverá atividades de avaliação e análise no âmbito do processo de avaliação e certificação do produto/serviço [NOME DO PRODUTO/SERVIÇO];

b)

c)

É celebrado o presente **ACORDO DE REGULAÇÃO DA CONFIDENCIALIDADE E DA PROPRIEDADE INTELECTUAL RESULTANTE DO PROCESSO DE AVALIAÇÃO E CERTIFICAÇÃO**, submetido às seguintes cláusulas:

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

PRIMEIRA

(Objeto)

SEGUNDA

(Conhecimento Prévio)

TERCEIRA

(Confidencialidade)

QUARTA

(Propriedade Intelectual)

QUINTA

(Vigência e Vicissitudes)

SEXTA

(Resolução de litígios)

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Feito em duplicado em _____, ficando cada parte com um exemplar, a [DATA].

_____

Pelo Gabinete Nacional de Segurança

_____

Pela EMPRESA

(PREENCHER - NOME)

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO I – Formulário de Candidatura de Organismos de Avaliação da Conformidade

O Formulário de pedido para início ou manutenção da prestação de serviços de avaliação da conformidade qualificados consta de 6 partes:

1 - Dados identificativos da pessoa coletiva ou sigular:

Pessoa:	Singular:	
(marcar com x)	Coletiva:	

[preenchimento geral]	
Denominação Social/Nome:	
Endereço (Sede):	
Código Postal:	
Localidade:	
E-Mail:	
Telefone:	
Endereço Internet:	
N.I.F:	

[apenas para Pessoa Colectiva]	
N. Pessoa Colectiva:	
Objecto Social:	
Corpos Sociais:	
Conservatória Registo Comercial:	
N.º Matrícula:	
Data Matrícula:	

2 - Declaração e assinaturas: Preencher os necessários.

Declaro que todos os dados fornecidos neste formulário estão corretos.	
Data:	
Local:	
Nome representante legal do Organismo Candidato:	
Assinatura:	

3 - Lista detalhada de documentos anexos a este formulário:

Preencher a tabela com identificação dos documentos identificados em 5.1. Documentação obrigatória.

Referência	Nome do documento

4 - Requistos de Confidencialidade, Independência e Imparcialidade: Preencher a tabela seguinte com todos os dados necessários e possiveis.

Requistos	Aplicável	Documento
Confidencialidade	SIM	

Deve anexar uma cópia da proposta de acordo de confidencialidade a celebrar caso seja necessário, e os documentos que comprovem que a entidade cumpre os requistos de imparcialidade necessários.

Requistos	Aplicável	Tipo	Documentos
Independência	SIM		
Imparcialidade	SIM		

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

5 - Identificação do(s) produto (s) a que se candidata: Colocar uma cruz (x) no tipo de serviços de confiança disponibilizados.

Classe Produtos	Categoria Produto	Tipo de Produto	Requisito de OAV	Sim (X)
Produtos Comerciais Não Criptográficos	Produtos de comunicações móveis seguras	Dispositivos móveis	EN ISO/IEC 17020	
		Aplicações móveis		
	Produtos físicos de computação	Estação de trabalho fixa		
		Estação de trabalho portátil		
		Produtos de preservação digital		
	Produtos de rede	Firewall		
		Data Diode		
		VPN Gateway		
		Exchange Gateway		
		Cross-Domain		
	Produtos de autenticação	Produtos Simples		
		Produtos de Multi-Factor autenticação		
	Produtos especificos de utilização Governamental	SmartCards	EN ISO/IEC 17025	
		Produtos Rádio	EN ISO/IEC 17020	
		Produtos Audiovisuais		
		Sistemas Operativos e Hipervisores		
Produtos Criptográficos	Módulos Cripto	HSM-T	EN ISO/IEC 17025	
	Produtos Criptografia de armazenamento	Encriptação de Ficheiro		
		Encriptação de Disco		
	Produtos Criptografia de Transmissão	Cripto Layer 2		
		Cripto Layer 3		
	Produtos de Gestão de Chaves	Tokens	EN ISO/IEC 17020	
		Vaults		
Produtos Baixa Radiação (TEMPEST)	Tipo A	Produtos de criptografia	EN ISO/IEC 17025	
		Produtos de rede		
		Produtos físicos de computação		
		Produtos rádio		
		Produtos audiovisuais		
	Tipo B	Produtos de criptografia		
		Produtos de rede		
		Produtos físicos de computação		
		Produtos rádio		
		Produtos audiovisuais		
	Tipo C	Produtos de criptografia		
		Produtos de rede		
		Produtos físicos de computação		
		Produtos rádio		
		Produtos audiovisuais		
Serviços de Computação em Nuvem	Infrastruture as a Service (IAAS)	Infraestrutura de serviços - Datacenter	EN ISO/IEC 17020	
	Platform as a Service (PAAS)	Plataforma de serviços - Máquinas Virtuais		
	Software as a Service (SAAS)	Aplicações de software - Produtos Software		
	Third Party Applications	Aplicações feitas por outras entidades para serem integradas em Serviços de Computação em Nuvem		

6 - Outras informações/observações: Redação livre sobre aspectos considerados relevantes para o processo.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO J – Modelo de Relatório de Avaliação Técnica

Capa do relatório:

LOGOTIPO

<NOME DA SUA EMPRESA>

Relatório de Avaliação Técnica (RAT)

<Nome do produto>

MODELO

Produto:	<Nome do produto>
Entidade Candidata:	Entidade Candidata
Organismo de Avaliação:	
Tipo de Avaliação:	
Avaliador(es):	

Referência/versão	<Referência e versão do documento>
Encontro: Data	<Data do documento>

COMERCIAL
CONFIDENCIAL

versão1.0

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Informações do documento

Identificação de documentos e projetos

Nome	Descrição
Título do documento	
Referência/versão	
Versão documento	
Tipo de avaliação	
Entidade Candidata	
OCC	
Organismo de Avaliação	

Histórico de versões

Versão	Data	Natureza da modificação	Página

Edição

<Nome dos redatores do documento>

Aprovação

<Nome e cargo do aprovador, data de aprovação, visto>

Difusão

<Lista de difusão>

Confidencialidade e aviso de direitos autorais

<Qualquer menção específica às regras de confidencialidade e aviso de direitos autorais>

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Introdução

Objetivo do documento

O Relatório de Avaliação Técnica padrão [RAT] contém informações proprietárias que não podem ser tornadas públicas. Este documento foi compilado para fornecer informações suficientes para o processo de certificação do <Nome do produto (TOE)>. Ele contém informações sobre a avaliação do TOE e deve permitir que o leitor entenda as ameaças e a eficácia das contramedidas. Este documento foi escrito de acordo com o documento referenciado [COMP].

Identificação do produto avaliado

A revisão avaliada do produto é:<Nome do produto>.

<Adicione qualquer detalhe útil à referência principal do produto, a fim de fornecer todas as informações necessárias para identificar claramente o produto durante a avaliação composta:

- Identificação do componente de hardware;
- Identificação de todas as bibliotecas de software incluídas;
- Identificação de possível plataforma de software incluída. >

Essas referências são fornecidas com as seguintes regras:

<Descreva as regras do fabricante para entender as referências fornecidas: referência comercial, referência técnica possível referência de plataforma de software, referências de bibliotecas de software, referências de peças de hardware (referência de cada conjunto de máscaras, identificação do local de produção…), identificação da lista de configuração completa [CONF] etc...>.

Identificação do perfil de proteção utilizado

A revisão avaliada foi feita com o perfil de proteção: <Nome do perfil de proteção>.

<Adicione com detalhe a referência ao perfil de proteção utilizado para avaliar o produto, a fim de fornecer todas as informações necessárias para identificar claramente quais os testes realizados e as exceções caso existam:

- Tabela com a identificação do perfil de proteção utilizado e possíveis comentários a cada linha/teste realizado >.

Descrição da documentação entregue

<Adicione a identificação e descrição sumária dos documentos entregues pela entidade responsável pela avaliação, assim como de todos os equipamentos ou produtos disponibilizados pela mesma entidade no âmbito da presente avaliação.>

Descrição do TOE

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Conceção geral

O produto é uma <descrição sumária do produto> projetada pelo <entidade candidata ou desenvolvedor> e construído em <detalhe sobre o tipo de tecnologia usado/fornecido>.

As principais características do produto estão representadas na figura 1:

<EXEMPLO>

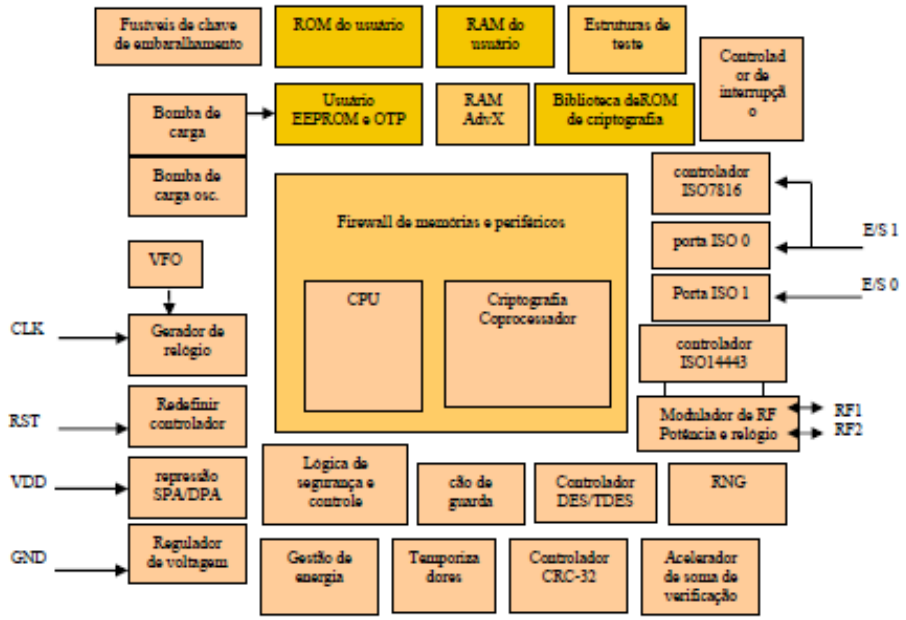

Figura 1 – Microcontrolador seguro

Podendo ser descrito através de:

- Uma parte de hardware, constituída por:

  - Uma unidade de processamento X-bit;
  - Memórias: EEPROM (<tecno e tamanho, possível mecanismo integrado>, para programa e armazenamento de dados), ROM (<tamanho>, <tamanho para software dedicado: Autoteste, bibliotecas criptográficas,…>) e RAM (<tecno e tamanho , possível mecanismo integrado>);
  - Módulos de Segurança: Lógica de Controle de Acesso à Memória, gerador de clock, administrador de segurança, gerenciamento de energia, controle de integridade de memórias;
  - Módulos funcionais: temporizadores de 8 bits, gerenciamento de E/S em modo contato (ISO 7816) e modo sem contato (ISO 14443), geradores de números aleatórios verdadeiros, unidades de coprocessamento DES e RSA….
  - …..

-Uma parte de software dedicado que compreende:

- Capacidades de teste do microcontrolador;

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

- Recursos de gerenciamento de interface de sistema e hardware/software;
- Recursos de gerenciamento de interface ISO 14443;
- Bibliotecas criptográficas: T-DES, AES e RSA, SHA2,….
- ….

O software integrado do cartão inteligente não faz parte da avaliação.

</EXEMPLO>

Descrição da estrutura TOE

<Esta parte depende da abordagem da Entidade Candidata ou desenvolvedor para descrever o *High Level Design* do produto.

Este capítulo deve conter uma lista de cada subsistema ou módulo do produto>.

<EXEMPLO>

Subsistema	Mecanismo de segurança	Tipologia:	Depende de:	Descrição, observações
SS14	Contramedidas SPA/DPA	Tecnologia	SSA14.2	Geração de relógio, com contramedidas como jitter, roubo de ciclo. Esses mecanismos devem ser ativados pelo software embarcado
…				
M.15	Hardware DES/TDES	Biblioteca	M15.1.1	Coprocessador DES de hardware. Não pode ser alterado porque faz parte completamente da lógica da cola
…				

Tabela 2- Projeto arquitetura

Legenda:

- Subsistema: referência ao subsistema ou módulo;
- Mecanismo de segurança: título do mecanismo de segurança [pode ser mesclado com a coluna anterior];
- Tipologia: para ser selecionado entre “tecnologia, recurso, design ou biblioteca de software”;
- Depende de: identificação de dependência logica ou física ou outra;
- Descrição, observações: descrição do mecanismo de segurança e a proteção fornecida para combater a ameaça ou parte da ameaça.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

</EXEMPLO>

Avaliação

Avaliação dos Requisitos gerais do Esquema

O conteúdo apresentado neste relatório é o resultado da avaliação realizada ao produto <Nome do produto> conforme especificado no Esquema de Certificação em Segurança Tecnológica e no perfil de proteção de segurança [<Nome do perfil de proteção>].

<Adicione possíveis comentários e histórico sobre reavaliação e referência do produto certificado anterior, RAT anterior e reutilização de tarefas.>

<Descreva a forma como os requisitos gerais foram declarados e as evidencias observadas sobre os mesmos, comprovando ou não que os mesmo se encontram cumpridos.>

Avaliação de Requisitos de Funcionalidade

<Descreva os testes realizados, a sua metodologia e os resultados obtidos>

Ameaça	Requisito funcional	Resultado	Impacto	Recomendação
T.NETWORK_EAVESDROP	FCO_VOC_EXT.1.1	FALHA	Potentially critical,…	Update to….
T.TSF_CONFIGURATION	FMT_SMF.1.1	OK	N/A	N/A
….	…	…	…	…
…..	…	…	…	…

Avaliação do nível de garantia

<Descreva as evidências recolhidas, a sua metodologia e os resultados obtidos >

SAR	Requisito	Resultado	Impacto	Recomendação
ALC.DEV.1.1	…….	FALHA	Potentially critical,…	Update to….
-----	……	OK	N/A	N/A
….	…	…	…	…

Avaliação do Nível de Proteção

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

<Descreve os mecanismos de segurança implementados por defeito e os mecanismos de segurança opcionais de cada produto, cálculo do rácio e resultado >

Resultados da Avaliação

<O objetivo deste capítulo não é repetir o processo de avaliação anteriormente descritos, mas delinear aspetos sensíveis que devem ser analisados com cuidado.

Fornecer um quadro resumo sobre a avaliação dos diversos requisitos a qualquer informação adicional necessária para um uso seguro.>

Lista de evidências

<O objetivo deste ponto é colocar numa tabela as evidências recolhidas e que levaram ao resultado da avaliação.>

Lista de ferramentas utilizadas

<O objetivo deste ponto é descrever as ferramentas que foram utilizadas na avaliação, o seu âmbito e utilização.>

Resultado final

<O objetivo deste ponto é dar conta do resultado global atingido pela avaliação.>

Conclusões e Recomendações

<O objetivo deste capítulo é dar conta do processo e do resultado final, identificando recomendações que podem ser utilizadas para melhorar o produto.>

Conclusão

<EXEMPLO>

O TOE submetido à avaliação não compreende nenhuma aplicação específica: não há software embarcado em ROM. No entanto, a ROM das amostras de avaliação contém um sistema operacional que permite aos avaliadores usar um conjunto de comandos com a E/S e carregar em software de teste EEPROM (ou em RAM). Este software não é avaliado: está fora do perímetro de avaliação (ou seja, nenhuma análise de vulnerabilidade é realizada nele).

As suposições para cada uma das fases de implementação do produto devem ser descritas e atendidas.

</EXEMPLO>

Recomendação

< O objetivo deste ponto é estabelecer linhas de orientação para a utilização segura do produto em função da conclusão, devendo existir uma tabela com todas as recomendações existentes.>

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

<EXEMPLO>

As premissas para as diferentes fases do produto descritas na meta de segurança devem ser verificadas no contexto da composição.

Da última observação surge uma recomendação para testes mais específicos: A análise de vulnerabilidades em software embutido ROM (além das bibliotecas criptográficas) deve ser realizada, pois esta questão não pode ser totalmente avaliada pela avaliação em dispositivos "genéricos".

Testes de penetração delinearam vulnerabilidades típicas de dispositivos de silício (particularmente EEPROM e sensibilidade de RAM à luz pulsada).

</EXEMPLO>

Parecer Final

<O objetivo deste capítulo não é repetir informação anterior, mas delinear aspetos importantes e conclusivos do processo de avaliação.

Forneça um parecer pragmático e assertivo sobre o resultado do processo de avaliação, evitando subjetividade e ambiguidades>

Devem constar como anexo, pelo menos, os modelos de seguida apresentados, a saber:

Anexo w - Configuração do produto avaliado

Anexo x - Perfil de Proteção utilizado

Anexo y - Orientações para uso do produto na sua configuração avaliada

Anexo z - Lista de documentos do produto

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Anexo w – Configuração do produto avaliado

ID	ITEM	Versão
1	Platform	
1.1	AP, AP/CP One(BB) Chipset	
1.1.1	AP, AP/CP One(BB) Chipset (Vendor/Series)	SEC | S5E9830(Exynos 990)
1.1.2	AP Chipset # of core	Octa-Core
1.1.3	AP Chipset Clock (GHz)	2.73GHz,2.5GHz,2GHz
1.1.4	AP Chipset Architecture(32/64bit)	64bit
....	.....	.....

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Anexo x – Perfil de Proteção utilizado

Classe	**Requisito de Segurança funcional**	**Nome**
Security audit (FAU)	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
Communications (FCO)	FCO_VOC_EXT.1.1	Fixed-rate Vocoder
…..	….	…

Classe	**Requisito de garantia de segurança**	**Nome**
Development (ADV)	ADV_FSP.1	…
	ADV_FSP.2	…
	ADV_FSP.3	…
….	….	…

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Anexo y – Orientações para uso do produto na sua configuração avaliada

Requisitos de Segurança	Ameaça	Impacto	Recomendações	Prioridade (0-5)
[AGD-2]				
…				

Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

Anexo z – Lista de documentos do produto

ID	Nome	Data	Versão
[AGD-1]			
[AGD-2]			
…			
[CERTIFICADO]			
[CONFIGURAÇÃO]			
[RAT]			
[ST]			
…			

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO K – Conteúdo da candidatura à certificação ou de notificação de alteração de um produto

O formulário de candidatura à certificação de um produto pode também ser utilizado para notificar alterações de produtos já previamente certificados.

O OCC deverá disponibilizar site online com a opção de efetuar uploads de ficheiros em formato pdf com tamanho, pelo menos, de 20 MB, para submissão da documentação.

O formulário deverá conter:

Secção 1: Identificação da Entidade Requerente e do produto candidato.

- Identificação da entidade responsável: (Nome, número de identificação fiscal e morada da sede).
- Contacto da entidade: (Identificação do ponto de contacto da entidade que irá ser responsável pelo acompanhamento do processo de certificação).
- Identificação do produto candidato: (Nome do produto).
- Nível de garantia (Nível de garantia para a qual o produto se pretende candidatar a avaliação: "Básico", "Melhorado" ou "Superior".
- Tipo de atividade associada à avaliação: Candidatura para concessão da certificação, renovação, etc.

Secção 2: Declaração de compromisso

Declaração do representante legal da EReq que confirma que a informação constante no presente formulário descreve corretamente produto candidato.

Secção 3 - Declaração de sigilo comercial

Deverá ser identificada a informação que no âmbito do processo de avaliação, são considerados sujeitos a sigilo comercial ou protegidos por direitos de propriedade intelectual ou industrial.

Secção 4: Relatório final de avaliação técnica e Plano de Correções (caso exista).

Secção 5: Manual de Procedimentos de Segurança (SecOps) do produto.

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698

ANEXO L – Modelo do Certificado de Conformidade

PRESIDÊNCIA DO CONSELHO DE MINISTROS
AUTORIDADE NACIONAL DE SEGURANÇA

CERTIFICADO DE CONFORMIDADE

[Nome do Produto ou Serviço]

Nos termos do disposto na alínea f) do n.º 2 do artigo 4.º do Decreto-Lei n.º 3/2012, de 16 de janeiro, republicado pelo Decreto-Lei n.º 136/2017, de 7 de novembro, ***certifico*** *que os, dispositivos/plataformas/aplicações/serviços adiante discriminada(s), foram avaliadas em termos de [* ***identificação do framework de avaliação seguido*** *] e cumprem os requisitos nacionais de segurança definidos para o processamento de informação classificada na marca e grau [* ***colocar marca e grau*** *].*

O presente certificado atesta ainda que os dispositivos/plataformas/aplicações/serviços a seguir discriminados são elegíveis para o processamento e transmissão de informação classificada até [***colocar marca e grau*** *] em* ***[descrição do contexto de utilização]*** *por um período* ***[colocar validade]****, a contar da data de emissão do presente Certificado, desde que [* ***identificação de condições específicas para a correta exploração/caveats (caso existam)]****.*

A utilização dos dispositivos/plataformas/aplicações/serviços a seguir discriminados para o processamento e transmissão de informação classificada [***colocar marca e grau*** *], requer a* ***acreditação*** *do sistema de informação e comunicação (SIC) subjacente a essa utilização por parte da Autoridade Nacional de Segurança nos termos do disposto na alínea f) do n.º 2 do artigo 4.º do Decreto-Lei n.º 3/2012, de 16 de janeiro na sua redação atual.*

Lisboa, xx de xxxxx de xxxxx

A Autoridade Nacional de Segurança

Nrº Certificado:
Lista de produtos:

GNS Gabinete Nacional de Segurança PORTUGAL
Rua da Junqueira, N.º 69 - 1300-342 LISBOA. E-mail: geral@gns.gov.pt TEL: + 351 21 040 36 00 FAX: + 351 21 040 3698