NT – B 01
24MAR2023

# NORMA TÉCNICA – B 01

## INSTRUÇÃO DOS PROCESSOS CONDUCENTES À ACREDITAÇÃO DE SEGURANÇA DOS SISTEMAS DE INFORMAÇÃO E COMUNICAÇÃO (SICs)

Lisboa, 24 de março de 2023

A Autoridade Nacional de Segurança

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2023.03.23 09:09:58 Z

(António Gameiro Marques)

(verso em branco)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

# 1. REFERÊNCIAS

a. Nacionais:

1) Lei Orgânica do GNS, aprovada pelo Decreto-Lei nº 3/2012 de 16 de janeiro com a Redação que lhe foi dada pelo Decreto-Lei nº 136/2017 de 06 de novembro;
2) Resolução do Conselho de Ministros nº 50/88, de 3 de dezembro (SEGNAC 1);
3) Resolução do Conselho de Ministros nº 37/89, de 24 de outubro (SEGNAC 2);
4) Resolução do Conselho de Ministros nº 16/94, de 22 de março (SEGNAC 3);
5) Resolução do Conselho de Ministros nº 05/90, de 28 de fevereiro (SEGNAC 4).

b. NATO:

1) C-M(2002)49 - NATO Security Policy;
2) AC/35-D/2004 – Primary Directive on CIS Security;
3) AC/35-D/2005 – Management Directive on CIS Security;
4) AC/35-D/1021 – Guidelines for the Security Accreditation of CIS;
5) AC/35-D/1017 – Guidelines for the Security Risk Management of CIS;
6) AC/35-D/1015 – Guidelines for the Development of Security Requirements Statements (SRSs);
7) AC/35-D/1014 – *Guidelines for the Structure and Content of Security Operating Procedures* (SecOPs) for CIS;
8) AC/35-D/1039 – Guidelines on Business Continuity Planning for CIS;
9) AC/35-N(2015)0022 (CISS) – Rules of Engagement for Security Audits of NATO CIS;
10) AC/35-D/2001REV3 - Directive on Physical Security;
11) AC/322-D/0047 - Directive on Cryptographic Security and Cryptographic Mechanisms;
12) AC/322-D/0048-REV3 (INV) – Technical and Implementation Directive on CIS Security;
13) AC/322-D/0049 - Directive for Transmission Security;
14) AC/322-D(2019)0021 (INV) - Directive on Emission Security;
15) AC/322-D/0030 - Directive for the Interconnection of CIS;
16) AC/322-D(2004)0030 - Directive on the Requirements for, and the Selection, Approval and Implementation of, Security Tools (ST).

c. União Europeia:

1) DECISÃO DO CONSELHO de 23 de setembro de 2013 relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE (2013/488/UE);
2) DECISÃO (UE, Euratom) 2015/444 DA COMISSÃO de 13 de março de 2015 relativa às regras de segurança aplicáveis à proteção das informações classificadas da UE;
3) DECISÃO (UE, Euratom) 2017/46 DA COMISSÃO de 10 de janeiro de 2017 relativa à segurança dos sistemas de comunicação e de informação na Comissão Europeia;

4) Information Assurance (IA) Security Policy on Security Throughout the CIS Life Cycle – IASP-L;
5) IA Security Policy on Security Governance – IASP-G;
6) IA Security Policy on Risk Management – IASP 1;
7) IA Security Policy on Cryptography – IASP 2;
8) IA Security Policy on Interconnection – IASP 3;
9) IA Security Policy on Network Defence – IASP 4;
10) IA Security Policy on CIS Security Engineering – IASP 5;
11) IA Security Policy on Qualification and Approval of non-cryptographic Products – IASP 6;
12) IA Security Policy on TEMPEST – IASP 7.

d. Outras:
1) SDIP 27 – NATO TEMPEST Requirements and Evaluation Procedures;
2) SDIP 28 – NATO Zoning Procedures;
3) SDIP 29 - Facility Design Criteria and Installation of Electrical Equipment for Processing Classified Information;
4) SDIP 30 – Installation of Electrical Equipment for the Processing Classified Information.

## 2. DEFINIÇÕES

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

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

c. **Acreditação de Segurança:**[3] Autorização formal para a exploração de um dado sistema, emitida pela Autoridade Nacional de segurança, com base no resultado de um processo de

[1] Tradução livre do documento "GUIDELINES for the SECURITY EVALUATION and CERTIFICATION of communication and information systems (CIS) - AC/35-D/1019-REV1"
[2] Idem
[3] Tradução livre do documento "GUIDELINES for the SECURITY ACCREDITATION of communication and information systems (CIS) - AC/35-D/1021-REV3"

avaliação, tendo em vista um dado propósito, como seja, o processamento de informação classificada. Incide sobre as entidades produtoras, consumidoras e disseminadoras de Informação Classificada (IC).

## 3. CONCEITOS

a. **Conceito de "*Security by Design*"[4]**: Abordagem de segurança sobre um produto TIC desde a sua conceção, procurando projetar padrões de segurança de forma holística, criativa, proactiva, interdisciplinar, robusta, responsável e integrada no desenho da arquitetura. É tida como o oposto de "segurança através da obscuridade".

b. **Conceito de "*Security by Default*"[5]**: Abordagem à configuração de produtos, serviços ou processos TIC, que garante a utilização por defeito de uma configuração segura, mesmo não sendo a mais fácil de utilizar, podendo ser definidas por normas ou referenciais extraídos de uma Análise do Risco e/ou de Testes de Verificação.

c. **Sistemas de Informação (SI)[6]**: Conjunto de componentes (Hardware e Software) inter-relacionados que trabalham em conjunto para recolher, processar, armazenar e distribuir informação para suporte da tomada de decisão, coordenação, controlo, análise e visualização numa organização.

d. **Sistemas de Informação e Comunicação (SIC)[7]**: Designam um qualquer sistema de informação e de comunicações que permite o tratamento de informação em formato eletrónico, que compreende todos os ativos necessários para seu funcionamento, incluindo a infraestrutura, a organização, o pessoal e os sistemas de informação (SI).

---

[4] 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;

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

[6] Tradução livre de LAUDON, K. e LAUDON, J., Essentials of Management Information Systems, Organization and Technology, 2nd edition, Prentice-Hall, 1996

[7] Tradução livre de COUNCIL DECISION of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU), disponível em: https://eur-lex.europa.eu/legal-content/EN/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=ENTXT/PDF/?uri=CELEX:32013D0488&from=EN, consultada em 17/08/2020;

## 4. SITUAÇÃO

a. A utilização de Sistemas de Informação e Comunicação (SIC), para o processamento de informação classificada, carece de uma acreditação por parte da Autoridade Nacional de Segurança.

b. A documentação em referência estabelece, para cada marca, as políticas e os critérios a seguir para a Acreditação de Segurança dos diversos SIC, nos múltiplos contextos em que podem ser operados.

c. Com a crescente proliferação de ameaças, torna-se essencial acautelar o risco inerente à exploração de SIC, assim como dos procedimentos de segurança implementados pelas diversas entidades, sendo essencial mitigar e nivelar o risco residual para um valor aceitável por todas as partes envolvidas no processo de Acreditação de Segurança.

d. Tendo por base que os processos de Acreditação de Segurança acompanham não só a adoção de SI, assim como, o ciclo de vida dos SIC, importa estabelecer os procedimentos para que em função do nível de ameaça, o processamento e disseminação de informação classificada pelas vários SIC, seja feita de forma expedita, mas controlada.

## 5. OBJETO/FINALIDADE

O presente documento tem como objetivo definir o processo de Acreditação de Segurança de um SIC habilitado a processar informação classificada.

## 6. ÂMBITO

A presente norma aplica-se a todas as entidades e organismos que utilizem SIC para o processamento de informação classificada de qualquer marca ou grau, em qualquer cenário ou ambiente e durante qualquer período de tempo.

## 7. PROCESSO DE ACREDITAÇÃO DE SEGURANÇA

a. O Gabinete Nacional de Segurança (GNS), no âmbito das atribuições expressas no Decreto-Lei n.º 3/2012, de 16 de janeiro, na sua redação atual, procede à acreditação de segurança de produtos e sistemas de comunicações, de informática e de tecnologias de informação que sirvam de suporte ao tratamento, arquivo e transmissão de informação classificada, em consonância com os organismos internacionais de que Portugal faz parte.

b. O processo de acreditação de segurança é aberto a qualquer entidade, independentemente da sua dimensão, atividade ou eventual associação com outros grupos ou instituições, de

natureza pública ou privada, com ou sem fins lucrativos, desde que cumpra os requisitos de acreditação correspondentes a cada marca e grau de segurança.

c. O GNS disponibiliza os seus serviços de acreditação de segurança a todas as entidades de uma forma imparcial e não discriminatória. Não obstante o GNS, reserva-se o direito de rejeitar candidaturas a qualquer entidade, cujos proprietários ou seus representantes, anteriormente tenham comprovadamente praticado atos lesivos do nome e/ou da imagem do GNS e/ou do funcionamento e credibilidade do processo de acreditação.

d. O processo de acreditação de segurança está sempre sujeito às orientações emitidas pela Autoridade de Acreditação de Segurança (SAA), presentes nas suas normas técnicas, devendo ser solicitado através de ofício conforme anexo C ao presente documento.

e. O Certificado de Acreditação determina o grau de classificação de segurança máximo de Informação classificada (IC) que pode ser armazenada, transferida e processada pelo SIC e os termos e condições correspondentes.

## 8. OBJECTIVOS DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA

O processo de Acreditação de Segurança, visa:

- A proteção da informação classificada manuseada por meios eletrónicos;
- O desenvolvimento de um processo de análise do risco de segurança ao longo do ciclo de vida de um SIC;
- A constituição de uma cadeia de confiança entre as diferentes entidades envolvidas no processo de acreditação de segurança;
- A implementação e atestação de uma arquitetura de segurança, que vise o cumprimento das políticas, diretivas e as normas técnicas de apoio pertinentes;
- A avaliação das medidas de segurança implementadas e mantidas, de acordo com os requisitos de segurança, incluindo a confirmação por meio de testes, análise de vulnerabilidades e inspeções de segurança apropriadas, de que as medidas de segurança dos SIC são implementadas e executadas em conformidade;
- A aferição da documentação de segurança relacionada com o SIC.

## 9. DESEMPENHO DE FUNÇÕES

a. Por forma a ir de encontro aos objetivos acima identificados, o processo de Acreditação de Segurança, requer ao nível organizacional a identificação de múltiplas funções.

b. Neste sentido, o Gabinete Nacional de Segurança, no âmbito das atribuições expressas no Decreto-Lei n.º 3/2012, de 16 de janeiro, assegura as funções de Autoridade de Acreditação de Segurança, vulgo *Security Accreditation Authority* (SAA) em Portugal, competindo-lhe:

- fornecer aconselhamento e orientação sobre política e diretivas de segurança da informação e medidas de segurança de apoio a entidades publicas e privadas;
- estabelecer um processo de acreditação de segurança, estabelecendo claramente as condições de acreditação de segurança para os SIC sob a sua autoridade, assim como, para as ligações e interligações de SIC externos a esses sistemas;
- revisar e aprovar a documentação relativa à segurança, planos de acreditação de segurança, relatórios de gestão do risco de segurança, SRSs (declarações de requisitos de segurança), arquiteturas de segurança, documentação de verificação de implementação de segurança e SecOPs (Procedimentos Operacionais de Segurança) e demais documentação nacional equivalente relacionada à segurança;
- revisar a documentação adicional, tais como conceitos de operação, relatórios de certificação de produto, manuais de instalações e guias de utilizador;
- fornecer um certificado de acreditação de segurança para o SIC, (conforme anexo E), indicando o período máximo de validade e as condições em que é exigida a reacreditação de segurança. Quando uma declaração de acreditação de segurança provisória é fornecida, a declaração deve identificar as condições a serem aplicadas à acreditação de segurança provisória e as atividades necessárias para obter a acreditação de segurança definitiva;
- verificar a aplicação das disposições de segurança para o SIC sob a sua responsabilidade, através de auditorias de segurança e principalmente através da realização de inspeções ou análises periódicas de segurança de acordo com o processo de acreditação de segurança;
- orientar as entidades, quando aplicável, no que diz respeito a avaliações de risco de segurança, gestão contínua de risco e aceitação de riscos residuais;
- fornecer orientação ao CISPIA, CISP, CISOA sobre a gestão de pessoal e a investigação de qualquer violação, ou suspeita de violação, das disposições de segurança, assim como, na avaliação dos danos causados;
- fornecer aconselhamento/recomendações sobre medidas corretivas a serem implementadas (ou recomendar fontes para aconselhamento apropriado);
- aconselhar o CISPIA, CISP e CISOA sobre o risco de segurança e as implicações das contramedidas de quaisquer alterações propostas ao SIC acreditado;

- exercer a supervisão do CISP e CISOA em relação à exploração do SIC e os resultados de ST&VP e atividades relacionadas à auditoria de segurança;
- manter contato com outros SAA no que diz respeito a SIC interconectados, para fins como acordar Declarações de Requisitos de Segurança de Interconexão de Sistema (SISRS) ou equivalente nacional;
- fornecer aconselhamento sobre a interconexão de SIC da NATO e outros SIC que tratam informação classificada;
- quando um SIC for obrigado a usar determinados produtos certificados, estabelecer ligação e coordenação com o CISPIA e as entidades internacionais apropriadas.

c. Tomando por base os documentos em referência é igualmente necessário que cada organização identifique as seguintes funções:

- **Responsável pela Governança do Sistema**, regularmente designado por Communication and Information Systems Planning and Implementation Authority (**CISPIA**);
- **Responsável Operacional do Sistema**, também designado por Communication and Information Systems Operational Authority (**CISOA**);
- **Responsável pela Manutenção do Sistema**, também conhecido por Communication and Information Systems Provider (**CISP**);
- **Oficial de Segurança do Sistema**, melhor conhecido por Communication and Information Systems Security Officer (**CISSO**);
- **Administrador do Sistema**, também conhecido por Communication and Information Systems Administrator (**CISADMIN**).

d. Neste sentido, e no âmbito da gestão de projetos, recomenda-se que cada Organização responsável por um SIC crie uma "Comissão de Gestão", composta por elementos com diferentes responsabilidades para elaboração e aprovação organizacional dos documentos integrantes do processo de acreditação de segurança.

e. Na medida em que compete a cada entidade um conjunto específico de funções, conforme seguidamente descritas.

f. O **CISPIA** é a entidade organizacional responsável pela orientação, planeamento e implementação de sistemas de informação e de comunicação a quem compete:

- desenvolver o SAP (Estratégia de Acreditação de Segurança) e submetê-lo ao SAA para sua aprovação;
- estabelecer os aspetos técnicos e operacionais de implementação do SIC, em conjunto com o CISP, CISOA e demais equipas/comissões constituídas para o projeto;

- aconselhar o CISP nos aspetos técnicos e de implementação sobre as alterações propostas para a configuração do SIC;
- aceitar as propostas de alteração aos requisitos operacionais ou mudança do nível da classificação da informação manuseada;
- garantir a transposição dos requisitos de segurança da informação (por exemplo, requisitos de segurança de rede e de sistema operacional, requisitos de componentes de fronteira, requisitos de prevenção contra software malicioso, etc..) em requisitos operacionais do SIC;
- definir os restantes requisitos a observar para os recursos de segurança do SIC a serem utilizados pela operação do SIC.

g. O **CISOA** é a entidade organizacional operacionalmente responsável pela exploração do SIC, a quem compete:

- definir os requisitos operacionais do serviço, princípios operacionais e conceito de operação do SIC, incluindo os requisitos referentes aos vários fluxos de informação considerados;
- manter contato, quando aplicável, com o CISPIA e o CISP durante o desenvolvimento do processo de avaliação de risco de segurança para o SIC, a fim de fornecer os dados para a avaliação e definir requisitos específicos de maturidade;
- aceitar formalmente o risco residual, quando aplicável, resultante do processo de avaliação do risco de segurança e chegar a acordo sobre um plano para gerir o risco residual. Com a exclusão das circunstâncias excecionais, não deve aceitar um nível de risco superior ao considerado aceitável pela SAA;
- assegurar que são estabelecidos níveis de serviço (SLA) ou mecanismos semelhantes com o CISP para a prestação dos serviços em exploração, designadamente no que diz respeito a requisitos de implementação, operação, monitorização e gestão de alterações das medidas de segurança;
- proceder à avaliação operacional do SIC e validar a sua autorização para utilização operacional, uma vez concedida a acreditação de segurança pela SAA;
- colaborar com a SAA na investigação de violações ou suspeitas de violação de segurança no SIC em exploração.

h. O Responsável pela Manutenção do Sistema (**CISP**) é a entidade organizacional responsável pela manutenção e correto provimento do SIC, a quem compete:

- formular, e manter sob revisão, a informação relacionada com a segurança do SIC;
- preparar a documentação exigida pela SAA em relação ao SIC sob a sua responsabilidade;

- apresentar propostas sobre as medidas de segurança do SIC a serem implementadas, em estreita cooperação e consulta com a CISPIA, e assegurar que as medidas de segurança do SIC acordadas são implementadas;
- estabelecer, o mais cedo possível no ciclo de vida do SIC, os recursos necessários para cumprir as funções de gestão da segurança do SIC no dia-a-dia;
- garantir que sejam tomadas medidas para uma formação adequada e apropriada em matéria de segurança da informação na fase inicial do ciclo de vida do SIC;
- fornecer à SAA as evidências exigidas para que a acreditação de segurança possa ser realizada de forma eficaz e solicitar a reacreditação de segurança de acordo com os requisitos do processo de acreditação de segurança;
- operar e apoiar as medidas de segurança de informação implementadas de acordo com as condições da acreditação de segurança dada;
- verificar, periodicamente ou em tempo real, a implementação das medidas de segurança garantindo que a postura de segurança do mesmo é consistente com os requisitos da SAA.

i. O Oficial de Segurança do Sistema (**CISSO**) é o elemento nomeado, a quem compete:

- garantir a correta implementação e manutenção das medidas de proteção no ambiente de segurança em que o SIC está localizado e que podem influenciar a postura de segurança da organização;
- verificar os respetivos certificados de acreditação de segurança de quaisquer SIC em uso, por forma a garantir que estes se encontram autorizados e mantenham o respetivo status de acreditação de segurança apropriado;
- garantir que todo o pessoal com acesso ao SIC possui conhecimento dos regulamentos de segurança e a autorização de segurança adequada ou esteja sempre acompanhado;
- garantir a realização de auditorias regulares de segurança para verificar se as medidas de segurança são implementadas e mantidas de acordo com os documentos de segurança aprovados e todas as demais diretivas de apoio.
- providenciar para que toda a informação classificada seja marcada e registada quer na entrada, como na expedição;
- garantir o controlo permanente do manuseamento e circulação interna da informação classificada, assegurando-se da sua salvaguarda durante e depois das horas de serviço;
- planear a evacuação e destruição de emergência, assegurando a oportuna disponibilização dos meios necessários para o efeito;

- fiscalizar a preparação, arquivo, guarda, transferência e expedição das informações classificadas;
- examinar e controlar a destruição de rascunhos, minutas, papéis químicos, fotocópias não utilizadas, cópias estragadas ou desnecessárias e demais desperdícios, de forma a assegurar que, através deles, não possam ocorrer comprometimentos ou quebras de segurança;
- propor a classificação de segurança, a reclassificação e a desclassificação, a informações produzidas pela organização, bem como a sua correção, quando for caso disso;
- sugerir, sempre que considere pertinente, as alterações a introduzir em quaisquer documentos e publicações eventualmente referentes a temas sensíveis, a fim de evitar que possam, inadvertidamente, ser revelados dados que se devam manter salvaguardados;
- colaborar na elaboração das cláusulas de segurança para contratos e subcontratos empreendidos pela organização, propondo a sua atualização, sempre que tal se justifique.
- participar, imediatamente, ao CISOA, todas as quebras de segurança e comprometimentos de que tenha conhecimento ou simples suspeita, para que se possa proceder às necessárias investigações e consequente comunicação às entidades interessadas, nomeadamente à SAA;
- manter uma estreita ligação com os demais oficiais com responsabilidades no âmbito da segurança em todos os aspetos relacionados com a segurança;

j. O Administrador do Sistema (**CISADMIN**) é o elemento nomeado, a quem compete:

- Manter uma estreita ligação com o oficial de segurança (CISSO) em todos os aspetos relacionados com a segurança da informação;
- Auxiliar o CISSO na definição dos limites do ambiente de segurança e na designação de áreas seguras;
- Implementar os procedimentos de segurança no SIC conforme instruído pelo oficial de segurança CISSO;
- Criar, manter e excluir as contas de utilizador do SIC com base na orientação do Oficial de Segurança (CISSO);
- Implementar as melhorias e modificações de *hardware*, *firmware* e *software* no SIC de uma maneira que não enfraqueça a postura de segurança do mesmo;
- Garantir que os jornais diários de rastreabilidade de segurança do SIC (*logs* de auditoria) são criados, registados e mantidos;

- Monitorar o backup e a recuperação de informação relevantes para a segurança do SIC;
- Apoiar e dar assistência, sempre que necessário, a administradores locais, quando constituídos em sites remotos;
- Fornecer sugestões de melhoria no âmbito de segurança do SIC ao CISSO.

## 10. SEGURANÇA INDUSTRIAL

a. A Segurança Industrial habilita diferentes entidades privadas a manusear informação classificada através de meios eletrónicos.

b. A salvaguarda da informação classificada presente em empresas sob qualquer forma, incluindo a forma digital, é da responsabilidade do Encarregado de Segurança conforme definido na Norma Técnica C-01 do GNS.

c. O Encarregado de Segurança deve desenvolver a sua atividade em permanente e estreita ligação com o Gabinete Nacional de Segurança (GNS), o qual lhe prestará todo o apoio necessário.

d. O manuseamento de informação classificada por meios eletrónicos em empresas está sujeita a um processo de acreditação para o SIC em causa e na marca e grau necessário;

e. A acreditação de um SIC por parte de uma empresa não pode desvirtuar o processo e credenciação industrial, pelo que uma empresa não pode possuir um nível de credenciação industrial inferior ao nível de acreditação do SIC que possui para manusear informação classificada em formato eletrónico.

f. Sempre que uma entidade privada deseje manusear IC através de um meio eletrónico, deve previamente iniciar o processo de acreditação do SIC junto do GNS.

g. O processo de acreditação de SIC pertencentes a entidades privadas, vulgo empresas, pode assumir a tipologia: *Offline* ou *Online*.

h. O processo de acreditação de SIC para operação em modo *Offline*, requer a elaboração de um documento descritivo dos procedimentos implementados pela empresa para assegurar a segurança da informação classificada detida.

i. No Anexo F encontra-se disponibilizado um modelo de documentação para ser usado pelas entidades privadas, que requeiram a acreditação de SIC para operação em modo *Offline*.

j. O processo de acreditação de um SIC para operação em modo *Online*, segue o processo de acreditação descrito no ponto 11. do presente documento.

k. No Anexo D encontra-se descrita a informação pertinente para cada documento necessário ao processo de acreditação de um SIC para operação em modo *Online*.

l. Para além da elaboração documental o processo de acreditação de SIC, requer a realização de uma avaliação de segurança física e eletrónica, assim como, uma auditoria de segurança aos equipamentos que irão ser utilizados para manusear informação classificada.

## 11. CICLO DE VIDA DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DE UM SIC[8]

a. O ciclo de vida do processo de acreditação de segurança de um SIC é definido como sendo composto por quatro fases, designadamente:

- Fase 1: Justificação do Processo de Acreditação de Segurança do SIC;
- Fase 2: Engenharia de Segurança do SIC;
- Fase 3: Manutenção, Reacreditação e Suspensão da Acreditação de Segurança do SIC;
- Fase 4: Desativação e Encerramento do Processo de Acreditação de Segurança do SIC.

b. Um diagrama do processo de acreditação encontra-se no anexo A.

c. Para cada fase existe um conjunto de atividades que necessitam de ser desenvolvidas para que o processo de acreditação se consolide, a documentação associada se mantenha atual e os atores obtenham a confiança necessária no SIC em acreditação.

d. O grau de exigência processual pode variar, em função da complexidade do SIC, da rede de comunicação, do ambiente operacional e/ou do grau de segurança que se deseje alcançar.

e. Os critérios de acreditação constituem-se como os requisitos técnicos que as entidades devem cumprir para acreditar os seus SIC e manterem a sua acreditação válida.

f. As medidas de segurança implementadas devem ser proporcionais ao risco de comprometimento do SIC e ao grau de classificação da informação que nele é tratada.

g. O manuseamento de IC por meios eletrónicos deve ser sempre efetuado por produtos criptográficos aprovados pela Autoridade de Nacional de Segurança.

[8] Baseado no documento IA Security Policy on Security throughout the Communication and Information System (CIS) Life Cycle - IASP L (ST 16268/12)

## 11.1. FASE 1: JUSTIFICAÇÃO DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DO SIC

a. Esta fase visa promover e consolidar as necessidades organizacionais, funcionais e de segurança que o manuseamento de IC por meios eletrónicos exige, devendo-se desenvolver as seguintes atividades para justificar a necessidade e alcançar uma confiança razoável no sistema:

- **Atividade 1-01 – Definir as necessidades organizacionais e funcionais:** as necessidades organizacionais e funcionais listam os métodos utilizados (questionário, entrevistas...) para reunir os requisitos que o SIC deve/pode contemplar, devendo conter pelo menos as seguintes informações:
    - alcance;
    - requisitos de ligação e interligação;
    - nível de classificação;
    - requisitos de confidencialidade;
    - requisitos de integridade;
    - requisitos de disponibilidade;
    - requisitos de autenticação;
    - requisitos de não repúdio;
    - outras necessidades funcionais do serviço.

  O CISP e o CISOA devem levar em consideração o tipo de sistema pretendido e procurar responder às diferentes questões que se colocam como por exemplo: para, por quem, quando, onde, porquê e como será usado, devendo ter em linha de conta as necessidades funcionais atuais do serviço, assim como, as necessidades futuras passiveis de serem estimadas.

- **Atividade 1-02 – Definir o conceito de operações (ConOps):** esta atividade visa identificar e descrever o conceito aplicável à operação prevista para a utilização do SIC, tomando por base a perspetiva do utilizador final.

  O conceito de operações deve levar em conta a cultura e a estratégia da organização, assim como, os seus recursos, definindo igualmente as políticas e os requisitos legais que serão aplicadas ao sistema.

- **Atividade 1-03 – Avaliação inicial de riscos de segurança:** esta atividade faz a primeira avaliação do risco de segurança do sistema, tendo por objetivo identificar e documentar, do ponto de vista organizacional, os vetores de ataque e os riscos de segurança, através de uma avaliação que afira o impacto e a probabilidade de todos os cenários de risco identificados.

  Conteúdo obrigatório:

- ativos com seus requisitos funcionais;
- processos com seus requisitos funcionais.

- **Atividade 1-04 – Definir a arquitetura conceptual de referência:** deve ser criada uma arquitetura conceptual, baseada nos fluxos de informação e seus requisitos de segurança, com base ConOps anteriormente definido (CIS Description).

  A arquitetura conceptual deve conter os diagramas de blocos que representaem cada componente e seus relacionamentos com os demais componentes.

  A arquitetura conceptual deve ainda descrever todos os fluxos de informação entre os ativos, devendo cada fluxo ser caracterizado pelos seus requisitos de segurança.

- **Atividade 1-05 – Definir a Estratégia de Acreditação (SAP)**: após a conclusão das atividades anteriores, deve ser concretizada uma estratégia de acreditação para dar início formal ao processo de acreditação junto da SAA.

  A Estratégia de Acreditação deve dar conta não só do plano temporal, mas também das responsabilidades que competem a cada uma das entidades envolvidas.

- **Atividade 1-06 – Elaboração da primeira versão dos Requisitos de Segurança do Sistema (SSRS) e os Procedimentos Operacionais de Segurança (SecOPs) do mesmo**: Juntamente com a estratégia de acreditação deve ser desenvolvida a primeira versão do SSRS e das SecOPs concentrando-se nos requisitos de segurança aplicáveis aos processos e nos objetivos de segurança baseados no ConOps.

  O SSRS e as SecOPs devem ser elaborados conforme orientações da SAA, devendo ser suficientemente claro para que seja fácil de ler por todas as partes interessadas.

  Ambos os documentos devem ser classificados na respetiva marca e grau RESERVADO ou equivalente

b. Esta fase termina com a receção por parte da SAA da documentação acima descrita e aprovação da Estratégia de Acreditação de Segurança proposta.

## 11.2. FASE 2: ENGENHARIA DE SEGURANÇA DO SIC

a. O sistema deve ser preparado para satisfazer os requisitos técnicos definidos antes de ser autorizado a entrar em operação. Para alcançar uma razoável confiança no SIC e nos processos implementados, considera-se necessário desenvolver as seguintes atividades de engenharia de segurança:

- **Atividade 2-01 – Identificar as medidas e controlos de segurança necessários**: a arquitetura conceitual e os requisitos de segurança devem ser traduzido em medidas e controlos de segurança.

As medidas e controlos de segurança podem ser escolhidos dentro de um referencial comumente aceite pela SAA e a CISOA, devendo o seu conteúdo possuir uma listagem com referências e rastreabilidade às necessidades funcionais do serviço suportadas.

O CISOA deve certificar-se de que as medidas e controlos de segurança selecionados podem ser implementados pelo Provedor do Sistema, e fornecer as métricas que permitam verificar a eficiência das medidas e dos controlos de segurança selecionados.

A SAA deve verificar a conformidade das políticas de garantia de informação com os requisitos legais e as medidas e controlos de segurança.

- **Atividade 2-02 – Implementar as medidas e controlos de segurança**: as medidas e os controlos de segurança identificados devem ser totalmente implementados pela organização. Sem a completa implementação de medidas e controlos não será possível prosseguir o processo de acreditação, na medida em que a avaliação dos risco tende a tornar-se teórica e subjetiva.
- **Atividade 2-03 – Gerir o desenvolvimento do SIC**: a implementação do sistema deve ser acompanhada e aprovada por todas as partes interessadas, sendo particularmente necessário se, por exemplo, qualquer uma das seguintes atividades se encontrar planeada:
    - ligação não prevista;
    - tecnologias de virtualização;
    - tecnologias disruptivas;
    - tecnologias não dominadas pelo CISP.
- **Atividade 2-04 – Preparar os recursos para operar o SIC**: o orçamento, os equipamentos, a localização, o pessoal e o conhecimento devem de ser planeados e disponibilizados antes da exploração e durante todo o ciclo de vida do SIC.

  O planeamento de recursos deve considerar o ciclo de vida do SIC, devendo conter as condições detalhadas, assim como a garantia de aquisição ou de terceirização de recursos, se tal for possível.
- **Atividade 2-05 – Plano de testes de segurança do SIC**: a organização deve planear quais os testes de segurança que devem ocorrer durante o desenvolvimento do sistema de forma progressiva, assim como, os testes de segurança que garantem a implementação das medidas e controlo necessários.

  Os testes devem ser realizados para garantir que a postura de segurança do sistema é mantida quando o sistema for instalado, devendo incluir a segurança física, eletrónica e de garantia da informação, pessoal e documental.

  O CISOA deve propor ao SAA o conteúdo do plano de teste de segurança, para aprovação por esta última.

Devem ser tomadas como referência as SSRS e as SecOps, assim como, o modelo de Certificado de Conformidade (SoC), quando relevante.

- **Atividade 2-06 – Pedido de autorização para testes (AfT)**: com o plano de testes aprovado pela organização, antes do início da realização de testes por parte da organização ou de outra entidade, esta deve solicitar autorização para a sua realização à SAA, que deve acompanhar os testes para validar os resultados e mitigar os riscos identificados ainda na fase de desenvolvimento.

  A AfT especifica as condições em que é aprovado, nomeadamente a marca e o grau mais elevado da informação classificada que pode ser usada no teste, as condicionantes para o plano e o prazo máximo para a conclusão dos testes.

- **Atividade 2-07 – Validação das medidas e dos controlos de segurança**: esta atividade consiste no teste efetivo da eficácia dos controlos de segurança definidos pelo plano de testes.

  O teste deve ser baseado em metodologias e técnicas de validação acordadas, devendo a equipa de teste ter as habilidades adequadas para testar os controlos de segurança nos diferentes domínios (físico, eletrónico, pessoal, documental e informático).

  A organização deve incluir nesta atividade a realização de testes de vulnerabilidades e penetração, devendo qualquer falta ou impossibilidade de testar um dado controlo ser adequadamente destacado, reportado à CISOA.

- **Atividade 2-08 – Estabelecer a base de referência para a postura de segurança**: assim que o sistema estiver estável e seguro, as configurações de todos os equipamentos devem ser congeladas e relatadas como base de referência para efeitos de postura de segurança.

  A base de referência para efeitos de postura de segurança deve garantir que qualquer mudança só possa ser realizada com a aprovação da CISPIA e CISOA.

  Qualquer solicitação de mudança deve ser justificada por uma análise de riscos ou uma avaliação do impacto de segurança.

- **Atividade 2-09 – Dossier TEMPEST**: o dossier TEMPEST deve centrar-se nos requisitos mínimos para a proteção TEMPEST e equilibrar as contramedidas TEMPEST numa abordagem eficiente para evitar a possível interceção de emanações comprometedoras contendo IC, devendo ser composto por:
  - Relatórios de zoning das instalações TEMPEST;
  - Certificados de equipamentos TEMPEST;
  - Seleção e distribuição de equipamentos pelas salas;
  - Instalação e planeamento de Áreas de Segurança e Áreas Tecnicamente Seguras.

- **Atividade 2-10 – Plano Criptográfico**: o Plano Criptográfico visa identificar e definir os procedimentos de operação criptográfica para os produtos criptográficos utilizados na operação do Sistema.

  Os produtos criptográficos usados para a proteção da IC durante a transmissão devem ser aprovados pela SAA, devendo abranger todos os aspetos operacionais, desde a instalação, gestão de chaves, manutenção, requisitos de segurança física e de pessoal, necessários à operação segura destes produtos.

  Devem ser elaborados planos criptográficos separados para produtos criptográficos distintos.

  A CISOA é responsável pelo fornecimento do Plano Criptográfico.

- **Atividade 2-11 – Utilização de PKI**: o objetivo desta atividade é identificar e definir os procedimentos de operação da infraestrutura de chave públicas (PKI), designadamente o controlo da emissão de certificados digitais para proteção de dados, o fornecimento de identidades digitais exclusivas para utilizadores, dispositivos e aplicativos, e a tipologia e protocolos de comunicações seguras previstos.

- **Atividade 2-12 – Avaliação e Auditoria de Segurança**: O objetivo desta atividade é confirmar que as medidas e os controlos, assim como, sistemas operativos e as demais aplicações se encontram corretamente configurados, não apresentando vulnerabilidades críticas ou de alto impacto, por parte da SAA.

  Nesta fase poderão ser realizadas visitas técnicas ao(s) local(ais) no âmbito da segurança por forma a consolidar os vários dossiers do processo de acreditação e apoiar a conclusão da fase de Engenharia de Segurança do Sistema.

  Os resultados da avaliação de segurança e da auditoria de segurança, serão alvo de relatório e entram para o processo de gestão do risco.

  A avaliação de segurança será feita no âmbito da segurança física e visa confirmar a segurança dos espaços usados para manusear IC na marca e grau pretendido, seguindo os Procedimentos de Teste e Verificação (STV&P) aprovados.

  Por seu turno a auditoria de segurança visa validar as configurações de segurança, a precisão dos dados de gestão da configuração e o nível de vulnerabilidades de segurança existentes:

  - A auditoria de segurança pode ser realizada pelo CISOA ou por entidade por este contratada, desde que devidamente coordenado e autorizado pelo SAA;
  - O relatório de auditoria deve ser preparado pelo CISOA e apresentado ao SAA para aprovação;
  - O relatório de auditoria deve incluir o plano de mitigação a ser seguido, caso sejam identificadas vulnerabilidades;

- A existência de um plano de mitigação para vulnerabilidades críticas ou altas, determina a conceção de uma acreditação interina com duração máxima de 12 meses.

- **Atividade 2-13 – Reavaliação do risco de segurança:** o objetivo desta etapa é proporcionar a revisão do nível de ameaças, do valor dos ativos, das vulnerabilidades identificadas, do impacto das mesmas, identificando os controlos adicionais para reduzir o risco de segurança para um nível aceitável, levando em conta todos os riscos inerentes que podem ter sido introduzidos ao longo do processo de desenvolvimento do Sistema.

  A reavaliação do risco deve partir da avaliação inicial dos riscos identificados durante a Fase I, adicionar os riscos e as vulnerabilidades identificadas na Fase II e promover a identificação das medidas e controlos de mitigação correspondentes, dando conta da revisão final do risco e da assunção do risco residual, por parte da organização.

- **Atividade 2-14 – Revisão Final da Documentação Genérica**: o objetivo desta etapa é concluir a elaboração da documentação genérica do sistema, designadamente do SSRS e das SecOps, mas também da restante documentação que consolida a operação do sistema em acreditação, designadamente:

  - A Análise de Impacto e o Plano de Continuidade de Negócio (BIA & BCP);
  - O Plano de Resposta a Incidentes e a Desastres (DRP);
  - O Plano de Evacuação de Emergência;
  - O Plano de Destruição de Emergência.

  Devem ser observados os requisitos documentais expressos no anexo D, ao presente documento.

  Após receção dos vários documentos, a SAA deve rever toda a documentação de segurança e quaisquer documentos relevantes para a segurança do Sistema, avaliando a conformidade da solução de segurança proposta em relação às obrigações de segurança existentes.

- **Atividade 2-15 – Certificação da solução de segurança**: o objetivo da certificação da solução de segurança é por um lado validar a conformidade da solução para com os requisitos de segurança, de governança, e de arquitetura do Sistema, dando como aceite a documentação de segurança entregue pela organização em particular os relatórios de avaliação de segurança e de auditoria de segurança.

- **Atividade 2-16 – Decisão sobre o processo de acreditação de segurança**: o objetivo desta atividade é dar conta da decisão por parte da SAA em relação ao processo de acreditação.

  Compete à SAA proferir um dos seguintes despachos:

1) Negar a acreditação de segurança, o que implica identificar deficiências específicas e ações corretivas significativas;
2) Suspender uma acreditação de segurança existente, o que implica identificar falhas graves na organização, acompanhadas de vulnerabilidades e deficiências específicas que colocam em risco a IC processada pelo sistema;
3) Conferir um dos seguintes Certificados de Acreditação de Segurança.

- **Acreditação Interina –** Autorização conferida para a utilização de um SIC por um período de tempo limitado, num ambiente operacional onde nem todos os requisitos de segurança são atendidos. A autorização deve identificar claramente as condições em que é dada (por exemplo, medidas de mitigação ou funcionalidades reduzidas), as atividades a serem realizadas e concluídas para alcançar a Acreditação de Segurança (por exemplo, aprovação final da documentação relacionada com a segurança) e o prazo para reavaliação da Acreditação Interina.

  A acreditação interina não pode ser repetida sucessivamente mais do que duas vezes.

  A concessão de uma acreditação interina deve ser precedida de um plano de mitigação que assegure que serão desenvolvidos todos os esforços para mitigar as limitações presentes num período máximo de 12 meses.
- **Acreditação de Segurança –** Autorização conferida para a utilização de um SIC num ambiente operacional devidamente especificado e que reúne todos os requisitos de segurança necessários para a exploração de informação classificada, assim como as condições para que a acreditação de segurança permaneça válida. A validade de uma Acreditação de Segurança não deve exceder os 36 meses.

b. Para sistemas complexos, definidos por diferentes camadas (Tier's), considera-se prudente uma aproximação faseada em termos de acreditação para cada uma das camadas.

c. Esta fase termina com a decisão final sobre o processo de acreditação por parte da SAA, após receção da documentação final.

## 11.3. FASE 3: MANUTENÇÃO, REACREDITAÇÃO E SUSPENSÃO DA ACREDITAÇÃO DE SEGURANÇA DO SIC

a. Para que um SIC mantenha a sua acreditação válida, é condição necessária que o mesmo continue a manter as suas valências em cada ciclo de acreditação.

b. A acreditação de segurança é valida dentro do prazo de validade indicado no certificado e desde que não sejam efetuadas alterações de ordem estrutural ao sistema ou à configuração aprovada.

c. A reacreditação de segurança do sistema implica que sejam desenvolvidos os necessários procedimentos com 6 meses de antecedência em relação aos prazos de validade do processo de acreditação.

d. A reacreditação de um sistema tem por base o desenvolvimento das seguintes atividades por forma a manter a confiança no sistema:

- **Atividade 3-01 – Monitorização Continua e manutenção do sistema:** Esta atividade visa por um lado garantir que a postura de segurança do sistema permanece válida e que nenhuma alteração foi introduzida sem a avaliação adequada. E por outro que as eventuais novas ameaças se encontram mitigadas quer por via dos controlos e segurança já implementados, quer pela implementação de novos controlos de segurança.

  A Comissão de Gestão, quando constituída, deve acompanhar todas as solicitações de alteração, garantindo sempre que as mesmas serão analisadas pelo CISP e o CISOA e uma avaliação do risco será previamente elaborada.

  Sempre que existirem novos desempenhos de funções ou alterações á configuração aprovada deve ser feita uma atualização da documentação existente, designadamente do SSRS e SecOPs e submetida novamente para aprovação da SAA.

- **Atividade 3-02 - Testes a medidas e controlos de segurança:** Esta atividade visa testar a eficácia dos controlos de segurança definidos pelo SSRS. Os controlos de segurança selecionados e implementados devem ser anualmente testados, de acordo com o STV&P, para validar a sua eficácia, devendo a SAA ser informada do seu resultado.

- **Atividade 3-03 – Monitorização das premissas do sistema:** o objetivo desta atividade é garantir que as premissas que levaram às escolhas dos controlos de segurança, princípios e decisões ainda se encontram válidos.

  Quaisquer alterações à documentação aprovada devem nesta fase ser revistas e apresentadas à SAA para aprovação.

e. Caso não exista a confiança necessária no sistema a SAA pode suspender a acreditação de segurança do sistema.

f. A suspensão consiste na interrupção temporária do processo de acreditação de segurança do sistema e na proibição de manuseamento de IC pelo sistema em causa.

g. A suspensão pode ter um prazo mínimo de 3 meses e um prazo máximo de 12 meses.

h. A suspensão poderá ser aplicada em virtude de atos ou omissões lesivas da segurança da informação manuseada pelo sistema em causa, como sejam:

- A não comunicação de uma ou mais alterações a um dado SIC anteriormente acreditado com pelo menos 30 dias de antecedência.
- A não comunicação de incidentes de segurança ocorridos no prazo máximo de 5 dias.
- A existência de incidentes de segurança graves ou a suspeita de violações de segurança que envolvam entidades internacionais.

## 11.4. FASE 4: DESATIVAÇÃO E ENCERRAMENTO DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DE UM SIC

a. O processo de acreditação de segurança, para um dado SIC anteriormente acreditado, encerra quando uma dada entidade comunicar esta pretensão com pelo menos 30 dias de antecedência à SAA.

b. Para manter a confiança nos processos de *phase-out* de um SIC acreditado devem ser desenvolvidas as seguintes atividades:

- **Atividade 4-01 – Plano de realocação de componentes de acordo com o seu uso futuro:** Esta atividade visa garantir que a segurança da IC não seja comprometida quando o sistema for encerrado ou quando um equipamento precisar de ser removido.
  Para tal, uma lista de equipamentos com a sua futura alocação (arquivamento, transferência, destruição) deve ser produzida pelo CISP.
- **Atividade 4-02 – Libertação dos recursos do sistema:** O equipamento listado durante a atividade anterior deve, em função do destino de cada recurso, ser alvo de um certificado de transferência ou de destruição, por parte do CISOA ou CISP, com posterior entrega à SAA.
  Esta etapa termina com a entrega, pela entidade responsável pelo sistema acreditado de:
  - Plano de realocação de componentes;
  - Plano de abate de componentes.
- **Atividade 4-03 – Arquivo da última configuração:** Esta atividade garante que foi feito o arquivo da última configuração por parte do CISP e sinaliza a desativação do sistema.
  Esta etapa termina com a confirmação por parte da SAA que o sistema deixou de estar autorizado a processar IC.

## 12. ALTERAÇÕES AO CONTEXTO DA ACREDITAÇÃO DE SEGURANÇA E INTERLIGAÇÃO ENTRE DIFERENTES SIC ACREDITADOS

a. Sempre que uma entidade pretenda realizar uma ou mais alterações a um dado SIC anteriormente acreditado deve comunicar esta pretensão com pelo menos 30 dias de antecedência.

b. Semelhantemente, para iniciar o processo de interligação de um SIC acreditado a um outro SIC a entidade responsável deve comunicar a referida pretensão com pelo menos 30 dias de antecedência à SAA.

c. Para estabelecer uma interligação devem ser desenvolvidas as seguintes atividades:

- **Atividade I-01 – Justificação da Interligação (SISRS):** Esta atividade visa dar conta dos objetivos e dos requisitos de segurança que devem ser implementados com a interligação de um SIC acreditado, a outro SIC acreditado, descrevendo nomeadamente qual a marca e grau da informação a trocar, os tipos de serviços comuns etc.

  Tomando como referência as SSRS e as SecOPs de cada um dos SIC, o CISOA de cada um dos SIC deve propor a SAA o conteúdo do plano de interligação (SISRS) , para aprovação por esta última.

- **Atividade I-02 – Avaliação do Risco da Interligação:** o objetivo desta etapa é rever o nível de ameaças e o valor dos ativos e as vulnerabilidades, procurando identificar o impacto e os controlos adicionais que podem reduzir o risco , levando em conta todos os riscos inerentes que podem ter sido introduzidos pela interligação dos SIC.

  A avaliação do risco deve partir da avaliação dos riscos identificados durante a Fase II de cada um dos SIC acreditados, adicionar os riscos e as vulnerabilidades identificadas pela Interligação e produzir as medidas ou controlos de mitigação correspondentes.

- **Atividade I-03 – Revisão de SSRS e SecOPs:** após a revisão do risco da interligação, em particular, da determinação e assunção final do risco residual, a organização deve promover uma revisão geral da documentação afetada pela interligação, por forma a concluir e entregar a mesma à SAA.

- **Atividade I-04 – Decisão sobre a acreditação de segurança da interligação**: o objetivo desta atividade é dar conta da decisão por parte da SAA em relação ao processo de acreditação da interligação.

  O processo segue o acima referido na atividade 2-16.

## 13. ACREDITAÇÃO DE PONTOS DE ACESSO

a. Os pontos de acesso caracterizam-se por serem sistemas habilitados a processar informação classificada de reduzida dimensão (número máximo de terminais por entidade igual a um) que fazem parte de uma infraestrutura de rede que não depende de entidade que o explora, disponibilizando na maioria das vezes apenas serviços de correio eletrónico dedicados a uma comunidade especifica.

b. A acreditação destes sistemas requer a disponibilização de pelo menos o Manual de SecOPs por parte da entidade operacionalmente responsável, podendo esta utilizar os demais documentos de apoio existentes no seio da comunidade em causa;

c. É obrigatória a realização de uma nova avaliação de segurança física e eletrónica, assim como a auditoria de segurança aos terminais sujeitos a um processo de acreditação.

## 14. ACREDITAÇÃO EXTRAORDINÁRIA E TEMPORÁRIA

a. Espera-se a total conformidade com as disposições descritas na presente norma técnica. No entanto, reconhece-se que pode haver circunstâncias especificas e excecionais, em que não seja possível o cumprimento integral do processo de acreditação estabelecido.

b. Para estas situações, a SAA, pode conceder uma acreditação extraordinária, limitada no tempo, devendo para tal estabelecer as condições mínimas de segurança a observar na exploração do SIC, durante um determinado período de tempo máximo e para um cenário ou ambiente específico.

c. Constituem-se como exemplos destas situações a utilização de SIC acreditados, em exercícios ou missões temporárias.

d. A acreditação extraordinária e temporária requer a disponibilização de pelo menos a descrição do cenário e ambiente específico, assim como, o Manual de SecOPs por parte da entidade operacionalmente responsável;

## 15. REVISÃO DA PRESENTE NORMA

A manutenção da presente norma é da responsabilidade do Departamento de Segurança Digital, Tecnológica e de Infraestruturas, a quem cabe sempre que se tornar exigível ou a cada período de 5 anos proceder à sua revisão e atualização.

## 16. ACRÓNIMOS

AfT – *Approval for Test* / Aprovação para Testes;

ANS – Autoridade Nacional de Segurança;

BIA – *Business Impact Analysis* / Análise de Impacto no Negócio;

BCP – *Business Continuity Plan* / Plano de Continuidade de Negócio;

ConOps – Conceito de Operações;

CIS Description – *Communication and Information System Description* / Descrição do Sistema de Informações e Comunicações;

CISADMIN – *Communication and Information Systems Administrator* / Administrador do Sistema de Informações e Comunicações;

CISOA – Communication and Information Systems Operational Authority;

CISP – Communication and Information Systems Provider;

CISPIA – Communication and Information Systems Planning and Implementation Authority;

CISSO – Communication and Information Systems Security Officer;

CSRS – Declaração dos Requisitos Genéricos de Segurança;

DRP – Plano de Resposta a Incidentes e Desastres;

GNS – Gabinete Nacional de Segurança;

IC – Informação Classificada;

NT – Norma Técnica;

PKI – Public Key Infrastructure;

SAA – *Security Accreditation Authority* / Autoridade de Acreditação de Segurança;

SAP – *Security Accreditation Plan* / Plano de Acreditação de Segurança;

SecOPs – *Security Operating Procedures* / Procedimentos Operacionais de Segurança;

SI – Sistemas de Informação;

SIC – Sistemas de Informação e Comunicação;

SISRS – Declaração dos Requisitos de Segurança de Interligação;

SRA – Análise do Risco de Segurança;

SSRS – Declaração dos Requisitos Específicos de Segurança;

STV&P – Manual de Procedimentos de Teste e Verificação;

TEMPEST – Telecommunications Electronics Material Protected from Emanating Spurious Transmissions.

## 17. ANEXOS

Anexo A – Fluxograma do processo de acreditação de segurança de um SIC.

Anexo B – Tabela de responsabilidades organizacionais.

Anexo C – Pedido de Acreditação de um SIC.

Anexo D – Conteúdo a observar na documentação.

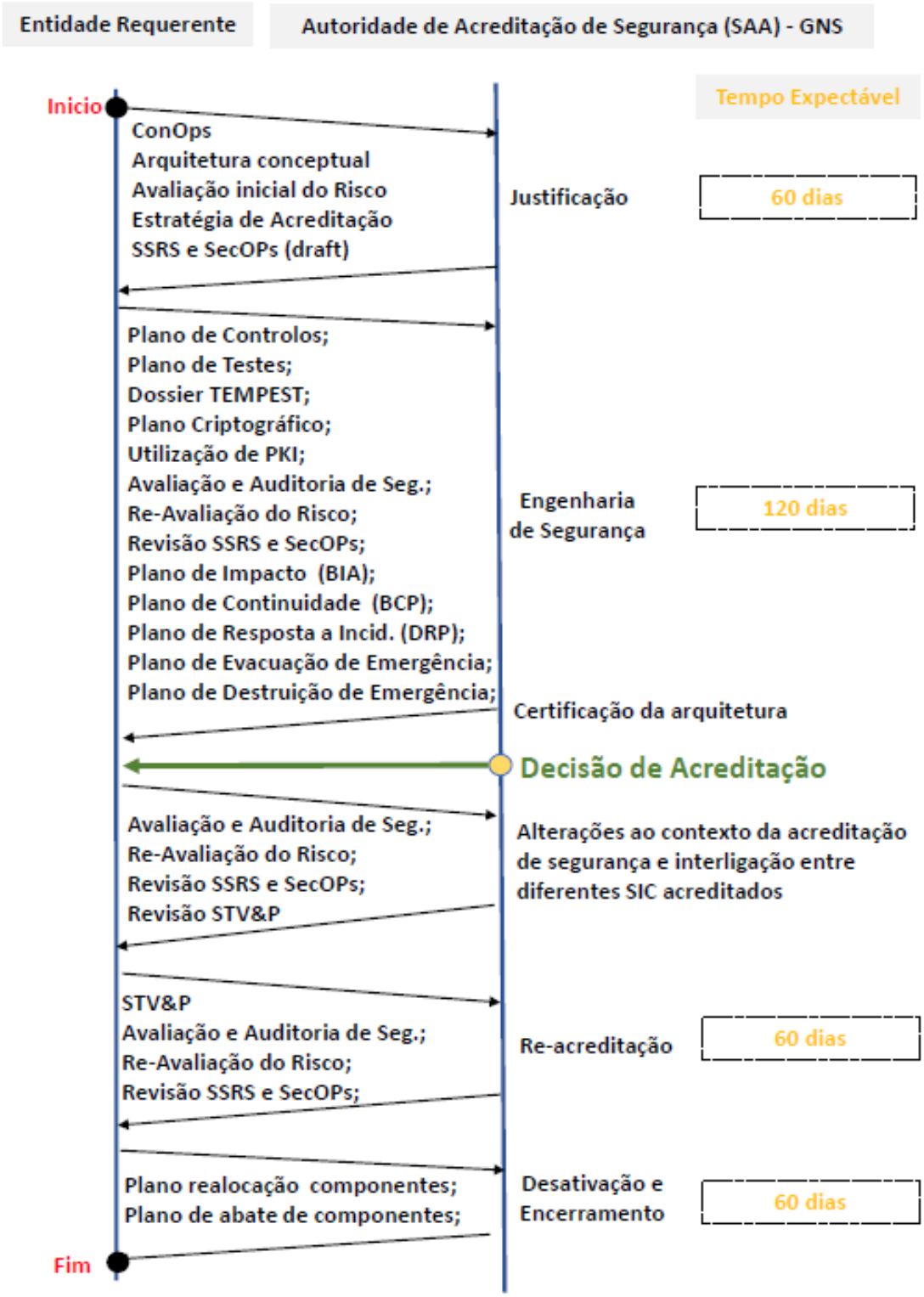
Anexo E – Certificado de Acreditação de Segurança.

Anexo F – Formulário para sistemas *Offline* pertencentes a entidades privadas.

## 18. LISTA DE DISTRIBUIÇÃO

Geral.

# ANEXO A – FLUXOGRAMA DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DE UM SIC



# ANEXO B – TABELA DE RESPONSABILIDADES ORGANIZACIONAIS

| Atividade | RACI | | | |
|---|---|---|---|---|
| | R | A | C | I |
| **JUSTIFICAÇÃO DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DO SIC** | | | | |
| Atividade 1-01 – Definir as necessidades organizacionais e funcionais: | CISPIA | CISPIA | CISOA | CISP |
| Atividade 1-02 – Definir o conceito de operações (ConOps) | CISOA | CISPIA | CISP | SAA |
| Atividade 1-03 – Avaliação inicial de riscos de segurança (SRA) | CISP | CISOA | CISPIA | SAA |
| Atividade 1-04 – Definir a arquitetura conceptual de referência (CIS Description) (Tier1 – Core; Tier 2 e Tier3) | CISP | CISOA | CISPIA | SAA |
| Atividade 1-05 – Definir a Estratégia de Acreditação (SAP) | CISPIA | SAA | CISOA | CISP |
| Atividade 1-06 – Elaboração da primeira versão do SSRS e SecOps | CISP | CISOA | SAA | CISPIA |
| **ENGENHARIA DE SEGURANÇA DO SIC** | | | | |
| Atividade 2-01 – Identificar as medidas e os controlos de segurança | CISP | CISOA | CISPIA/ SAA | - |
| Atividade 2-02 – Implementar as medidas e os controlos de segurança | CISOA | CISP | CISPIA/ SAA | - |
| Atividade 2-03 – Gerir o desenvolvimento do sistema | CISOA | CISPIA | SAA | - |
| Atividade 2-04 – Preparar os recursos para operar o SIC | CISOA | CISPIA | CISP | - |
| Atividade 2-05 – Plano de testes de segurança do SIC (STV&P) | CISOA | SAA | CISP | CISPIA |
| Atividade 2-06 – Pedido de autorização para testes (AfT) | CISPIA | SAA | CISOA | CISP |
| Atividade 2-07 – Validação das medidas e dos controlos de segurança | CISP | CISOA | CISPIA | SAA |
| Atividade 2-08 – Estabelecer a base de referência em termos de postura de segurança | CISP | CISOA | CISPIA | SAA |
| Atividade 2-09 – Dossier TEMPEST | CISP | CISOA | SAA | CISPIA |
| Atividade 2-10 – Plano Criptográfico | CISP | CISOA | SAA | CISPIA |
| Atividade 2-11 – Utilização de PKI | CISP | CISOA | SAA | CISPIA |
| Atividade 2-12 – Avaliação e Auditoria de Segurança | CISP | SAA | CISOA | CISPIA |
| Atividade 2-13 – Reavaliação do risco de segurança (SRA) | CISP | CISOA | SAA | CISPIA |
| Atividade 2-14 – Revisão Final da Documentação Genérica | CISP | CISOA | SAA | CISPIA |
| Atividade 2-15 – Certificação da solução de segurança | SAA | SAA | - | CISPIA/ CISOA |
| Atividade 2-16 – Decisão sobre o processo de acreditação de segurança | CISPIA | SAA | CISOA | CISP |
| **MANUTENÇÃO, REACREDITAÇÃO E SUSPENSÃO DA ACREDITAÇÃO DE SEGURANÇA DO SIC** | | | | |
| Atividade 3-01 – Monitorização continua e manutenção do sistema | CISP | CISP | CISOA | SAA |
| Atividade 3-02 - Testes a medidas e controlos de segurança | CISP | CISP | CISOA | SAA |
| Atividade 3-03 – Monitorização das premissas do sistema | CISPIA | SAA | CISOA | CISP |
| **DESATIVAÇÃO E ENCERRAMENTO DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DE UM SIC** | | | | |
| Atividade 4-01 – Plano de realocação de componentes de acordo com futuro uso | CISOA | CISP | CISPIA | - |
| Atividade 4-02 – Libertação de recursos do sistema | CISP | CISOA | CISPIA | SAA |
| Atividade 4-03 – Arquivo da última configuração | CISPIA | SAA | CISOA | CISP |

(verso em branco)

| OUTRAS SITUAÇÕES GERAIS: | | | | |
|---|---|---|---|---|
| **INTERLIGAÇÃO ENTRE DIFERENTES SIC ACREDITADOS** | | | | |
| Atividade I-01 – Justificação da Interligação (SISRS) | CISPIA | SAA | CISOA | CISP |
| Atividade I-02 – Avaliação do Risco da Interligação | CISP | CISOA | SAA | CISPIA |
| Atividade I-03 – Revisão de SSRS e SecOps | CISP | CISOA | SAA | CISPIA |
| Atividade I-04 – Decisão sobre a acreditação de segurança da interligação | CISPIA | SAA | CISOA | CISP |
| **ALTERAÇÕES AO CONTEXTO DA ACREDITAÇÃO DE SEGURANÇA** | | | | |
| Comunicar a pretensão sobre realizar uma ou mais alterações a um dado SIC anteriormente acreditado, com pelo menos 30 dias de antecedência. | CISP | CISPIA | CISOA | SAA |
| Comunicar todo e qualquer incidentes de segurança ocorridos no prazo máximo de 5 dias. | CISP | CISPIA | CISOA | SAA |
| **ACREDITAÇÃO EXTRAORDINÁRIA E TEMPORÁRIA** | | | | |
| Disponibilização da descrição do cenário e ambiente específico, assim como, o Manual de Procedimentos de Segurança (SecOPS). | CISPIA | SAA | CISOA | CISP |
| **ACREDITAÇÃO DE PONTOS DE ACESSO** | | | | |
| Disponibilização do Manual de Procedimentos de Segurança (SecOPS). | CISPIA | SAA | CISOA | CISP |
| **SEGURANÇA INDUSTRIAL** | | | | |
| Disponibilizar modelo de documentação, conforme Anexo F, para acreditação de SIC para operação em modo Offline. | Conselho Adminsitração | SAA | Encarregado Segurança | - |
| Seguir o processo de acreditação anteriormente definido, para tipologias Online. | Conselho Adminsitração | SAA | Encarregado Segurança | - |
| Comunicar a pretensão sobre realizar uma ou mais alterações a um dado SIC anteriormente acreditado, com pelo menos 30 dias de antecedência. | Encarregado Segurança | Conselho Adminsitração | - | SAA |
| Comunicar todo e qualquer incidentes de segurança ocorridos no prazo máximo de 5 dias. | Encarregado Segurança | Conselho Adminsitração | - | SAA |

**R (Responsável):** Entidade que executa uma atividade sendo responsavel pela apresentação do resultado a quem aprovou a atividade.
**A (Acionável):** Entidade que tem a responsabilidade final e autoriza a conclusão correta de uma ou várias atividades.
**C (Consultado):** Entidade que é consultada previamente e que para além de aconselhar, também auxilia na execução, aprova a linha de ação e orienta o resultado.
**I (Informado):** Entidade que é mantida informada com informação atualizada sobre o andamento e os resultados alcançados.

# ANEXO C – PEDIDO DE ACREDITAÇÃO DE UM SIC

**DE:** [Nome da entidade/empresa]

**PARA:** Diretor Geral do Gabinete Nacional de Segurança
Presidência do Conselho de Ministros
Rua da Junqueira, 69
1300-342 Lisboa

**ASSUNTO:** Solicitação de (re)acreditação do SIC [nome do sistema de informação]

1. [Nome da entidade/empresa] possui um SIC denominado ……..…… [nome do SIC], cujo propósito é ……. [breve descrição do propósito do SIC] sendo este constituído por …… [breve descrição do número de sites] e para o qual pretende processar informação classificada na marca …….. [indicar a marca] e grau …….. [indicar o grau máximo] a partir de …….. [data estimada de início de exploração]
2. Nesse sentido, [nome da entidade/empresa] solicita gentilmente o seu apoio para iniciar o processo de acreditação do referido SIC, necessitando da indicação de um ponto de contacto da sua organização.
3. O nosso ponto de contacto para este assunto é …… [nome e contacto do elemento da entidade requerente]

……. [local], ……. [data]

……..

[Assinatura]

(verso em branco)

# ANEXO D – CONTEÚDO A OBSERVAR NA DOCUMENTAÇÃO

a. Os documentos que instruem o processo de acreditação, doravante designados por peças, podem ser entregues de forma individual e desfasadas umas das outras, em língua portuguesa ou inglesa.

b. Sempre que possível devem ser usados formulários próprios ou adaptados para a execução das peças necessárias para o processo de acreditação, identificados em 6.e), de acordo com a marca e o grau que se pretende acreditar.

c. O desenvolvimento do processo de acreditação deve ir evoluindo através de versões de trabalho ("draft"), passiveis de poderem ser corrigidas e alteradas. Apenas a versão final deverá ser devidamente assinada por todas as partes.

d. Todas as peças devem conter: bloco de assinaturas; controlo de versões, controlo de cópias e índice.

e. O bloco de assinaturas deve conter: a assinatura de quem preparou (CISP/CISOA), de quem aprovou (CISOA/CISPIA) e de quem vai autorizar (SAA).

f. Dependendo da marca e grau de classificação do sistema em acreditação e em coordenação com a SAA, podem existir pequenas variações quer em termos de conteúdo, quer em termos dos documentos necessários para a conclusão do processo de acreditação.

g. Em situações em que é requerida a acreditação de segurança para uma marca e grau, para as quais não existem referências doutrinárias na SAA, compete à entidade requerente facilitar os contactos e a documentação necessária à SAA por forma a auxiliar a aferição das condições de segurança exigidas para essa marca e grau.

h. A avaliação documental consiste numa revisão da documentação, pela qual a arquitetura dos SIC é analisada para determinar a conformidade entre a configuração base definida pela entidade proponente e os requisitos de segurança definidos pela política de segurança para a marca e grau em causa (NACIONAL/NATO/EU/ESA), tendo por base a composição de cada documento a seguir discriminado.

i. O Conceito de Operações (ConOps), deve no mínimo incluir:

- Âmbito;
- Propósito;
- Necessidades do negócio em relação ao manuseamento de IC, com indicação da marca e grau da IC a manusear;

- Descrição do conceito de produção, manuseamento e arquivo de informação classificado pelo sistema proposto para acreditação;
- Descrição das funcionalidades e serviços associados ao sistema previsto;
- Pode ainda incluir:
  - Definição de um plano de recursos inicial;
  - Definição de uma organização de segurança.

j. A Arquitetura de Segurança do SI (Descrição do SIC), deve incluir, no mínimo:

- Âmbito;
- Pressupostos e assunções;
- Descrição da arquitetura a implementar (lógica e física);
- Diagrama global do SIC, diagrama lógico do "Core", diagrama lógico por Camadas (*Tiers*);
- Diagrama com identificação e composição das diferentes zonas de segurança, implementadas, nomeadamente:
  - Zona de fronteira;
  - Zona DMZ;
  - Zona de supervisão;
  - Zona de operação;
  - Zona "Core";
- Descrição dos fluxos de informação implementados pela arquitetura no que diz respeito a pelo menos as seguintes situações:
  - Identificação e autenticação;
  - Atualização e manutenção de segurança;
  - Registo e classificação de IC;
  - Processamento e armazenamento de IC;
  - Transferência e impressão de IC;
- Lista de serviços a disponibilizar incluindo a identificação de cada protocolo a usar e as respetivas portas de rede previstas;
- Lista HW (com identificação das certificações atribuídas);
- Lista SW (com identificação das certificações atribuídas).

k. O Plano de Acreditação de Segurança (SAP), deve no mínimo incluir:

- Âmbito;
- Descrição sumária do sistema proposto para acreditação;
- Propósito da acreditação, com indicação da marca e grau da IC a manusear;

- Definição de uma organização de segurança;
- Definição das responsabilidades de cada entidade pertencente à organização de segurança;
- Identificação da documentação, conforme a presente norma, e entidade primariamente responsável pela entrega da mesma;
- Definição e calendarização do processo de acreditação;
- Processo de acreditação de interligações (caso existam);
- Processo de manutenção da acreditação e de reacreditação;
- Processo de abate/substituição.

l. A Análise do Risco (SRA) deve determinar e identificar:

- Âmbito;
- Caracterização dos vários ambientes (caso existam);
- Identificação e caracterização de ativos por ambiente;
- Identificação e valorização das ameaças;
- Identificação e caracterização da maturidade dos mecanismos de segurança implementados em cada ambiente;
- Vulnerabilidades identificadas e valorizadas;
- Identificação do Risco Potencial e Risco Residual;
- Proposta de tratamento das principais ameaças identificadas;
- Conclusão e avocatura da responsabilidade pela entidade operacionalmente responsável pelo risco residual.
- NOTA:
    - O processo de gestão do risco tem por base uma matriz de ameaças, uma tabela de medidas de segurança e um nível de maturidade mínimo para cada medida de segurança dentro de cada Marca e Grau, sendo adotadas as referências existentes em cada momento para cada Marca e Grau para a condução do processo de acreditação.
    - A maturidade de cada organização ou comunidade, segue os conceitos de "Security by Design" e "Security by Default".

m. Os Requisitos Genéricos/Específicos de Segurança (CSRS/SSRS/SISRS) devem conter:

- Âmbito;
- Descrição sumária do SIC utilizado;
- Caracterização das instalações e do ambiente de segurança geral, local e eletrónico;

- Indicação da criticidade da informação, dos serviços e dos recursos usados;
- Lista de serviços disponibilizados por tipologia de instalação incluindo lista de portas de rede usadas por cada protocolo;
- Resumo de ameaças, impactos e riscos e requisitos legais;
- Identificação e caracterização dos requisitos e mecanismos de segurança implementados em termos de:
    - Segurança Física;
    - Segurança Pessoal;
    - Segurança Documental;
    - Segurança de Rede e Cibersegurança;
    - Segurança Eletrónica;
    - Segurança Criptográfica;
    - Segurança das Comunicações.
- Justificação para a não implementação de mecanismos de segurança mandatórios;
- Caracterização dos controlos de segurança implementados, nomeadamente no que diz respeito a:
    - Políticas da Organização;
    - Gestão do Risco;
    - Proteção de Hardware e de *Removable Storage Devices*;
    - Proteção de Software;
    - Proteção de Serviços;
    - Proteção dos Dados;
    - Proteção de Fronteira;
    - Segurança de Rede;
    - Segurança das Comunicações e Segurança das Emissões;
    - Segurança dos SI de Controlo;
    - Segurança de Pessoal;
    - Segurança Física e Ambiental;
    - Gestão de Identidade, Autenticação e Acessos;
    - Gestão da Configuração;
    - Supervisão, Monitoramento Contínuo e Auditoria;
    - Postura de Manutenção Segura;
    - Resposta a Incidentes;
    - Planeamento de Contingência;
    - Auditoria de Segurança e Teste de Verificação de Segurança;
    - Educação, Formação e Sensibilização sobre Segurança.

- Pode ainda incluir:
  - Definição de uma organização de segurança (caso não tenha sido feita noutro documento);
  - Definição de requisitos de segurança a observar nas interligações;
  - Avaliação genérica do risco;
  - Procedimento de teste e verificação de requisitos/mecanismos de segurança.
- Quando se tratar de Requisitos Específicos de Segurança para uma Interligação, deve incluir:
  - Descrição sumária da Interligação;
  - Caracterização em termos e redes IP utilizadas e serviços interligadas;
  - Indicação da criticidade da informação, dos serviços e dos portos usados por cada protocolo;
  - Avaliação do risco realizada sobre a interligação;
  - Declaração de conformidade assinada por ambas as CISOA de cada SIC.

n. O Manual de SecOPs deve incluir pelo menos:

- Âmbito;
- Pontos de contato de referência;
- Definição de procedimentos de criação de utilizadores, administradores e auditores de segurança, incluindo a de tomada de conhecimento e responsabilização individual a preencher por cada utilizador/administrador/auditor;
- Definição de procedimentos de exploração, registo e arquivo de dados;
- Definição de procedimentos de utilização de periféricos e dispositivos amovíveis de memória;
- Definição de procedimentos de acesso e impressão de informação classificada;
- Definição de procedimentos de introdução e extração de informação classificada;
- Definição de procedimentos de controlo de configuração;
- Definição de procedimentos de manutenção de segurança;
- Definição de procedimentos de auditoria e análise de vulnerabilidades;
- Pode ainda incluir:
  - Plano de Continuidade de Negócio;
  - Plano de Resposta a Incidentes e a Desastres.

o. O Manual de Procedimentos de Teste e Verificação (STV&P) deve incluir no mínimo:

- Âmbito;
- Definição do objetivo dos procedimentos de teste e forma como se completam;
- Identificação das ferramentas que devem ser utilizadas;

- Procedimentos de execução e repetição;
- Identificação e caracterização dos testes a realizar para cada um dos domínios descritos nos requisitos de segurança e em função de cada mecanismo de segurança implementado;
- Caracterizar a aplicabilidade de cada teste e a execução local ou central do mesmo;
- Resultado obtido para cada teste e justificação para os resultados negativos;
- Avaliação do risco resultante de cada resultado negativo, com indicação das medidas corretivas tomadas;
- Plano de mitigação para cada resultado negativo cujo tratamento não tenha sido possível fazer *in loco*.

p. A Análise de Impacto e o Plano de Continuidade de Negócio (BIA & BCP) deve incluir no mínimo:

- Âmbito;
- Identificação dos principais serviços/áreas de negócio;
- Identificação das funções críticas e fluxos de informação críticos;
- Identificação das dependências entre os vários serviços/áreas e as funções/fluxos de informação;
- Caracterização de cenários de ameaça e do tempo de inatividade aceitável para cada função crítica;
- Plano de resiliência para manter as operações nas seguintes dimensões:
    - Disponibilidade, Integridade e Confidencialidade, Autenticidade e Não Repudio;
- Pode ainda incluir:
    - Plano de Resposta a Incidentes e a Desastres.

q. O Plano de Resposta a Incidentes e a Desastres (DRP) deve incluir no mínimo:

- Âmbito;
- Apresentação Geral do Plano;
- Pressupostos;
- Exclusões e Exceções;
- Cenários de Ameaça e de Planeamento (incluindo a avaliação da probabilidade, o seu impacto e a estratégia de mitigação);
- Objetivos de Recuperação;
- Sequência Lógica de Eventos;

- Descrição das equipas de Gestão de Incidentes Locais e Centrais;
- Listas de Verificação para resposta a incidentes;
- Procedimentos de Notificação e Comunicação Interna e Externa;
- Procedimentos de Teste e Exercício;
- Pode ainda incluir:
    - Plano de Evacuação de Emergência;

r. O Plano de Evacuação de Emergência deve incluir pelo menos:

- Âmbito;
- Apresentação geral do plano e a sua relação com outros planos de evacuação, nomeadamente o plano de evacuação geral das instalações;
- Exclusões e Pressupostos;
- Cenários de Planeamento (incluindo a identificação das ameaças, a sua probabilidade, o seu impacto e a estratégia de mitigação);
- Sequência Lógica de Eventos;
- Descrição das equipas de Evacuação de Emergência (incluindo contatos);
- Listas de Verificação para Evacuação de Emergência;
- Procedimentos de Registo, Notificação e Comunicação Interna e Externa (incluindo listas telefónicas e contactos de emergência);
- Procedimentos de Teste e Exercício.

s. O Plano de Destruição de Emergência deve incluir pelo menos:

- Âmbito;
- Apresentação geral do plano e a relação com outros planos;
- Exclusões e Pressupostos;
- Cenários de Planeamento (incluindo a identificação das ameaças, a sua probabilidade, o seu impacto e a estratégia de mitigação);
- Sequência Lógica de Eventos;
- Descrição das equipas de Destruição de Emergência (incluindo contatos);
- Listas de Verificação para Destruição de Emergência;
- Procedimentos de Registo, Notificação e Comunicação Interna e Externa (incluindo listas telefónicas e contactos de emergência);
- Procedimentos de Teste e Exercício.

t. O Relatório de Avaliação de Segurança deve incluir pelo menos:

- Âmbito;
- Descrição do processo de avaliação de segurança efetuado;

- Identificação das ferramentas usadas e descrição das infraestruturas avaliadas;
- Apresentação de resultados da avaliação de segurança, tomando por base o Manual de Procedimentos de Teste e Verificação (STV&P), de forma compreensiva com indicação de vulnerabilidades e nível de severidade;
- Apresentação de outras evidências observadas de forma compreensiva com indicação da vulnerabilidades e nível de severidade;
- Plano de mitigação para cada vulnerabilidade cujo tratamento não tenha sido possível fazer *in loco*.

u. O Relatório de Vulnerabilidades deve incluir pelo menos:

- Âmbito;
- Descrição do processo de análise de vulnerabilidades efetuado;
- Identificação das ferramentas usadas e descrição do sistema avaliado;
- Apresentação de resultados da análise de vulnerabilidades de forma compreensiva com indicação do nível de severidade por vulnerabilidade;
- Avaliação do risco resultante de cada vulnerabilidade com indicação das medidas corretivas tomadas e a justificação sobre as vulnerabilidades pendentes;
- Plano de mitigação para cada vulnerabilidade cujo tratamento não tenha sido possível fazer *in loco*.

PRESIDÊNCIA DO CONSELHO DE MINISTROS
AUTORIDADE NACIONAL DE SEGURANÇA

# CERTIFICADO DE ACREDITAÇÃO DE SEGURANÇA

**Nr.º SIC:**
**NOME:**

Ref.:

a. C-M(2002)49 - Security within the North Atlantic Treaty Organization;
b. AC/35-D/1021 Guidelines for the Security Accreditation of Communication and Information Systems (CIS);
c. AC/322-D/0048-REV3 Technical and Implementation Directive on CIS Security
d. ACO Security Accreditation Strategy (SAS);
e. Etc...

Para os efeitos do disposto na alínea f) do n.º3 do artigo 2.º e alínea f) do n.º2 do artigo 4.º, ambas do Decreto-Lei n.º 3/2012, de 16 de janeiro na sua redação atual, certifico que o Sistema de Informação e Comunicações (SIC) acima identificado se encontra **acreditado** na marca e grau **XXXXXXXX XXXXXXX** de acordo com as referências acima descritas.

O presente certificado atesta que o SIC identificado está autorizado a manusear informação classificada na(s) marca(s) e grau(s) acima descrito(s), desde que mantenha as condições de segurança e o modo de operação descrito na documentação entregue por parte da **[Entidade responsável]**.

É responsabilidade da **[CIS Operational Authority]** garantir que o nível de risco que a exploração do SIC apresenta se mantem no nível baixo, devendo quaisquer violações dos regulamentos agora aceites ou controlos de segurança implementados ser devidamente investigados de acordo com as referências acima e reportadas à Autoridade Nacional de Segurança no prazo máximo de 5 dias.

Confirmo que será dado apoio para qualquer dúvida ou questão de segurança que se considere necessário, sendo desde já minha responsabilidade garantir a supervisão, auditoria e inspeção periódica do sistema explorado operacionalmente pela **[CIS Operational Authority]**.

A presente acreditação é válida por um período de 3 (três) anos, contando desde **xx de xxxxxxx de xxxx até xx de xxxx de xxxx.**

Lisboa, XX de XXXXXXXXX de XXXX

A Autoridade Nacional de Segurança

(Nome)

(verso em branco)

# ANEXO F – FORMULÁRIO PARA SISTEMAS STAND-ALONE PERTENCENTES A ENTIDADES PRIVADAS

LOGO Marca e grau do documento

PROCEDIMENTOS OPERACIONAIS DE SEGURANÇA PARA POSTOS DE TRABALHO ISOLADOS

Preparado por:

Aprovado por:

Autorizado por: (Pela Autoridade Nacional de Segurança)

LOGO2 com endereço Marca e grau do documento

(verso em branco)

## CONTROLO DE VERSÕES DO DOCUMENTO

| Versão | Data | Páginas | Alterações |
|---|---|---|---|
| 1.0 | 23/04/2021 | 46 | Versão inicial do documento |

## CONTROLO DE CÓPIAS E DISTRIBUIÇÕES

| Recipiente | Nº de Cópias |
|---|---|
| Gabinete Nacional de Segurança | 1 (one) |
| .... | ... |
| .... | ... |
| ... | |
| | |



(verso em branco)

# INDICE

1. INTRODUÇÃO ..... 6
1.1. OBJECTIVO ..... 6
1.2. ALCANCE ..... 6
1.3. DEFINIÇÕES E ACRÓNIMOS ..... 6
1.3.1. DEFINIÇÕES ..... 6
1.3.2. ACRÓNIMOS ..... 6
2. REFERENCIAS ..... 7
2.1. DOCUMENTOS APLICÁVEIS ..... 7
2.2. DOCUMENTOS DE SUPORTE ..... 7
3. PROCEDIMENTOS OPERACIONAIS DE SEGURANÇA ..... 9
3.1. ORGANIZAÇÃO DE SEGURANÇA ..... 9
3.2. MODO DE OPERAÇÃO ..... 10
3.3. DIAGRAMA DE REDE ..... 11
3.4. CONFIGURAÇÃO HARDWARE DO SISTEMA ..... 12
3.5. CONFIGURAÇÃO DO SOFTWARE DO SISTEMA ..... 13
3.6. SERVIÇOS DISPONIBILIZADOS PELO SISTEMA ..... 13
3.7. PROTOCOLOS E PORTOS ATIVADOS ..... 15
3.8. SEGURANÇA DO SIC ..... 16
3.8.1. SEGURANÇA DO SISTEMA OPERATIVO ..... 16
3.8.2. CONTROLO DE ACESSO ..... 16
3.8.3. ELIMINAÇÃO SEGURA ..... 17
3.8.4. RELATÓRIOS DE ACTIVIDADE. AUDITORIA ..... 17
3.8.5. SUPORTES REMOVÍVEIS ..... 18
3.8.6. PROTEÇÃO DA INFORMAÇÃO ..... 18
3.8.7. FERRAMENTAS DE SEGURANÇA ..... 19
3.8.8. SEGURANÇA CRIPTOGRÁFICA ..... 19
3.8.9. SEGURANÇA DE EMISSÕES ..... 20
3.9. GESTÃO DE SEGURANÇA ..... 20
3.10. SEGURANÇA FÍSICA ..... 21
3.11. SEGURANÇA DO PESSOAL ..... 21
3.12. SEGURANÇA DOCUMENTAL ..... 22
3.13. PLANO DE CONTINUIDADE DE NEGÓCIO ..... 22
4. ANEXOS ..... 24
4.1. FORMULARIO PARA O PEDIDO DE ACESSO OU MODIFICAÇÃO DO ACESSO AO SISTEMA ..... 24
4.2. FORMULARIO PARA A NOTIFICAÇÃO DE INCIDENTES ..... 26
4.3. DECLARAÇÃO DE CONHECIMENTO DOS PROCEDIMENTOS DE SEGURANÇA DOS POSTOS DE TRABALHO ISOLADOS ..... 28

4.4. SOLICITAÇÃO PARA INTRODUÇÃO DE DADOS EM MEIOS INFORMÁTICOS E SUPORTES REMOVÍVEIS COM INFORMAÇÃO CLASSIFICADA ..... 29

4.5. SOLICITAÇÃO PARA EXTRAÇÃO DE DADOS DOS MEIOS INFORMÁTICOS E SUPORTES REMOVÍVEIS COM INFORMAÇÃO CLASSIFICADA ..... 30

4.6. FORMULÁRIO DE PROPOSTA DE MODIFICAÇÃO HW/SW ..... 31

4.7. LISTA DE UTILIZADORES AUTORIZADOS COM CONTA DE UTILIZADOR NO SISTEMA ..... 32

4.8. LISTA DE DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEL AUTORIZADOS ..... 33

4.9. RELATÓRIO DE AUTO-AVALIAÇÃO DOS MECANISMOS DE SEGURANÇA IMPLEMENTADOS ..... 34

4.10. REGISTO DE ENTRADAS/SAIDAS DE POSTOS DE TRABALHO DA ÁREA DE SEGURANÇA DE CLASSE 142