FAQS – NT B 01

Lisboa, 8 de setembro de 2023

A Autoridade Nacional de Segurança

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2023.10.11 21:46:48 +01'00'

(António Gameiro Marques)

(verso em branco)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

(verso em branco)

QUE SISTEMAS DEVEM SER SUJEITOS A UMA ACREDITAÇÃO DE SEGURANÇA?

1. Qualquer sistema/equipamento ou serviço que permita o processamento de informação classificada por meios eletrónicos ou digitais, de qualquer marca e grau, igual ou superior a RESERVADO ou equivalente, em qualquer cenário ou ambiente e durante qualquer período de tempo.

2. Estão sujeitos a acreditação todos os ativos necessários, a infraestrutura, a organização, o pessoal e o conjunto de componentes (Hardware e Software) inter-relacionados que trabalham em conjunto para recolher, processar, armazenar e distribuir informação classificada para suporte da tomada de decisão, coordenação, controlo, análise e visualização numa organização.

O QUE É UMA AVALIAÇÃO DE SEGURANÇA?

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

O QUE É UMA CERTIFICAÇÃO DE SEGURANÇA?

A Certificação de Segurança é o processo 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).

O QUE É UMA ACREDITAÇÃO DE SEGURANÇA?

A Acreditação de Segurança é uma autorização formal para a exploração de um dado sistema, emitida pela Autoridade Nacional de Segurança, com base no resultado de um processo de avaliação e certificação tendo em vista um dado propósito e um dado contexto, como seja, o processamento de informação classificada. Incide sobre as entidades produtoras, consumidoras e disseminadoras de informação classificada (IC).

QUAIS OS OBJECTIVOS DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA?

O processo de Acreditação de Segurança, tem como objetivos:

- Assegurar a proteção da informação classificada manuseada por meios eletrónicos;
- Apoiar 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.

NO ÂMBITO DA ACREDITAÇÃO DE SEGURANÇA O QUE SE ENTENDE POR SISTEMA?

Sistema é o conjunto composto pela trilogia criada pela tecnologia, pessoas e processos.

O QUE É O CONCEITO "SECURITY BY DESIGN"?

Abordagem à segurança tecnológica de um produto TIC desde a sua conceção, procurando integrar em todo o processo de engenharia (desde o desenho, desenvolvimento, testes e manutenção) padrões e considerações de segurança de forma holística, criativa, proativa, interdisciplinar, robusta, responsável e integrada no desenho da respetiva arquitetura e desenvolvimento do produto. É uma abordagem completamente oposta à de "segurança por obscurantismo"[1]

O QUE É O CONCEITO "SECURITY BY DEFAULT"?

O conceito "Security by Default" é uma 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.

QUEM DEVE SOLICITAR A ACREDITAÇÃO DE SEGURANÇA?

O processo de acreditação de segurança deve ser aberto pelas entidades produtoras, consumidoras e disseminadoras de informação classificada (IC), sendo 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.

QUANDO DEVE SER SOLICITADA UMA ACREDITAÇÃO DE SEGURANÇA?

Deve ser solicitada com pelo menos 6 meses (180 dias) antes da data prevista para entrada em produção do Sistema de Informação e de Comunicação (SIC) sobre o qual se pretende a acreditação.

[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;

QUE SISTEMAS DEVEM SOLICITAR UMA ACREDITAÇÃO DE SEGURANÇA?

Qualquer sistema de informação e de comunicação (SIC) que permite o tratamento de informação classificada em formato eletrónico, compreendendo todos os ativos necessários para seu funcionamento, a infraestrutura, a organização, o pessoal e o conjunto de componentes (Hardware e Software) inter-relacionados que trabalham em conjunto para recolher, processar, armazenar e distribuir informação classificada para suporte da tomada de decisão, coordenação, controlo, análise e visualização numa organização.

QUAL O TEMPO EXPECTÁVEL QUE O PROCESSO DE ACREDITAÇÃO DE SEGURANÇA DEMORA?

Cerca de 180 dias (6 meses) após receção do pedido formal. Para um processo de Re-acreditação cerca de 120 dias (4 meses).

SERÁ NECESSÁRIO A ACREDITAÇÃO DE SEGURANÇA PARA SISTEMAS NACIONAIS NÃO CLASSIFICADOS?

Não é requerida a Acreditação de Segurança para sistemas de informação e comunicação (SIC) que processem informação NÃO CLASSIFICADA, não obstante recomenda-se que seja envolvido o Centro Nacional de Cibersegurança (CNCS), na medida em que possui um conjunto de boas práticas que podem auxiliar no desenho da arquitetura, implementação e configuração.

QUAL O CUSTO DO PROCESSO DE SEGURANÇA?

De acordo com a Tabela anexa à Portaria n.º 283/2014, 31 de dezembro, na sua redação atual, importa ter em conta que:

Serviços	TAXAS (Isentas de IVA)
Acreditações/Credenciações	
1 — Acreditação de segurança de redes e/ou sistemas de informação:	
Até 10 terminais, inclusive	2.000,00 €
Mais de 10 terminais	4.000,00 €
2 — Acreditação de centros de comunicações ou de centros de dados (segurança física e zoning)	1.500,00 €
3 — Acreditação de sites no âmbito do Projeto Galileo	1.000,00 €
4 — Acreditação de empresas no âmbito do serviço PRS do Projeto Galileo	500,00 €
….	
17 — Ação de zoning (medição e análise de radiação eletromagnética de equipamentos)	1.000,00 €

….	
19 — Auditoria a sistemas de informação	500,00 €/dia

(*) Os serviços prestados pelo GNS a micro, pequenas e médias empresas (PME) têm uma redução de 25% sobre o montante das taxas aplicáveis.

- (**) Estão isentos da aplicação de taxas os serviços prestados pelo GNS às forças e serviços de segurança, aos demais organismos que integram o Sistema de Informações da República Portuguesa e aos demais serviços da área governativa da Administração Interna.
- (***) Este montante não inclui a inspeção do respetivo órgão de segurança, que está associada ao processo de credenciação.
- (****) O montante da taxa relativa à prestação de serviço de credenciação, renovação e elevação de pessoas singulares (por marca) tem uma redução de 50%, sempre que o mesmo seja prestado às áreas governativas dos Negócios Estrangeiros e da Defesa Nacional, bem como às Forças Armadas.

O QUE PRECISO PARA SOLICITAR UMA ACREDITAÇÃO DE SEGURANÇA?

Fazer pedido no site do GNS em: https://www.gns.gov.pt/# ou enviar ofício ao Diretor Geral do Gabinete Nacional de Segurança com uma breve descrição do SIC que se pretende acreditar e a marca/grau pretendido, assim como, a identificação do ponto de contato para o processo de acreditação. O pedido através de ofício, poderá ser substituído por um pedido através do portal do GNS, com a disponibilização da mesma informação que para o ofício.

O QUE INCLUI O PROCESSO DE ACREDITAÇÃO DE SEGURANÇA?

O processo de acreditação de segurança inclui:

- Assessoria e consultadoria no desenho da arquitetura;
- Apoio na avaliação do risco;
- Auxílio no desenvolvimento do processo documental;
- Realização de uma auditoria de segurança física;
- O acompanhamento ou realização de uma auditoria de segurança da informação ao sistema;
- e a emissão de um Certificado de Acreditação que determina a marca e grau máximo da classificação de segurança da Informação classificada (IC) que pode ser manuseada pelo sistema.

QUANTAS FASES POSSUI O CICLO DE VIDA DO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA?

O ciclo de vida do processo de acreditação de segurança de um SIC é definido como tendo quatro fases, designadamente:

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

EM QUE FASE É SUPOSTO OBTER A ACREDITAÇÃO DE SEGURANÇA?

O ciclo de vida do processo de acreditação de segurança de um SIC é definido como tendo quatro fases. Para obter a acreditação de segurança é necessário completar a Fase 1 e Fase 2.

QUAIS AS ATIVIDADES QUE DEVEM SER DESENVOLVIDAS NA FASE 1?

As atividades que devem ser desenvolvidas na primeira fase são:

- Atividade 1-01 – Definir as necessidades organizacionais e funcionais;
- Atividade 1-02 – Definir o conceito de operações (ConOps);
- Atividade 1-03 – Avaliação inicial de riscos de segurança;
- Atividade 1-04 – Definir a arquitetura conceptual de referência;
- Atividade 1-05 – Definir a Estratégia de Acreditação (SAP);
- Atividade 1-06 – Elaboração da primeira versão dos Requisitos de Segurança do Sistema (SSRS) e os Procedimentos Operacionais de Segurança (SecOPs) do mesmo.

O QUE É O CONCEITO DE OPERAÇÕES (CONOPS)?

O conceito de operações (CONOPS) deve identificar e descrever o conceito aplicável à operação prevista para a utilização do SIC, tomando por base a perspetiva do utilizador final.
Deve ter 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, designadamente o cuidado a ter com o registo de informação classificada.
Neste sentido, deve 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, registo, 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.

QUAIS AS ATIVIDADES QUE DEVEM SER DESENVOLVIDAS NA FASE 2?

As atividades que devem ser desenvolvidas na segunda fase são:

- Atividade 2-01 – Identificar as medidas e controlos de segurança necessários;
- Atividade 2-02 – Implementar as medidas e controlos de segurança;
- Atividade 2-03 – Gerir o desenvolvimento do SIC;
- Atividade 2-04 – Preparar os recursos para operar o SIC;
- Atividade 2-05 – Plano de testes de segurança do SIC;

- Atividade 2-06 – Pedido de autorização para testes (AfT);
- Atividade 2-07 – Validação das medidas e dos controlos de segurança;
- Atividade 2-08 – Estabelecer a base de referência para a postura de segurança;
- Atividade 2-09 – Dossier TEMPEST;
- Atividade 2-10 – Plano Criptográfico;
- Atividade 2-11 – Utilização de PKI;
- Atividade 2-12 – Avaliação e Auditoria de Segurança;
- Atividade 2-13 – Reavaliação do risco de segurança;
- Atividade 2-14 – Revisão Final da Documentação Genérica;
- Atividade 2-15 – Certificação da solução de segurança;
- Atividade 2-16 – Decisão sobre o processo de acreditação de segurança.

QUAIS AS ATIVIDADES QUE DEVEM SER DESENVOLVIDAS NA FASE 3?

As atividades que devem ser desenvolvidas na terceira fase são:

- Atividade 3-01 – Monitorização Continua e manutenção do sistema;
- Atividade 3-02 - Testes a medidas e controlos de segurança;
- Atividade 3-03 – Monitorização das premissas do sistema.

QUAIS AS ATIVIDADES QUE DEVEM SER DESENVOLVIDAS NA FASE 4?

As atividades que devem ser desenvolvidas na terceira fase são:

- Atividade 4-01 – Plano de realocação de componentes de acordo com o seu uso futuro;
- Atividade 4-02 – Libertação dos recursos do sistema;
- Atividade 4-03 – Arquivo da última configuração.

COMO SÃO TRATADOS OS CASOS ESPECIAIS?

Para os casos especiais, a ANS 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 máximo e para um cenário ou ambiente específico.

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

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;

QUAIS OS RESULTADOS EXPECTÁVEIS DE UM PROCESSO DE ACREDITAÇÃO DE SEGURANÇA?

Espera-se que a certificação da solução de segurança valide 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.

O PROCESSO DE ACREDITAÇÃO DE SEGURANÇA INCLUI ALGUM TIPO DE AUDITORIA AO SISTEMA?

Sim. O Processo de acreditação inclui uma Auditoria de Segurança que 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 *Communication and Information Systems Operational Authority* (CISOA) ou por entidade por este contratada, desde que devidamente coordenado e autorizado pela *Security Accreditation Autority* (SAA).

O relatório de auditoria deve ser preparado pelo CISOA e apresentado ao SAA para aprovação e deve incluir o plano de mitigação a ser seguido, caso sejam identificadas vulnerabilidades.

QUAIS AS FUNÇÕES QUE DEVEM PARTICIPAR NO PROCESSO DE ACREDITAÇÃO DE SEGURANÇA?

O Processo de Acreditação requer que sejam identificadas as seguintes funções organizacionais por forma a estabelecer uma cadeia de confiança:

- Autoridade de Acreditação, regularmente designado por *Security Accreditation Autority* (SAA) é em Portugal desempenhada pela Autoridade Nacional de Segurança;
- 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).

QUAIS AS RESPONSABILIDADES DO CISP?

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 re-acreditação 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.

QUAIS AS RESPONSABILIDADES DO CISOA?

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.

QUAIS AS RESPONSABILIDADES DO CISSO?

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;

QUAL O CONTEÚDO A OBSERVAR NA DOCUMENTAÇÃO?

Os documentos que instruem o processo de acreditação de segurança, doravante designados por peças, podem ser entregues de forma individual e desfasadas umas das outras, em língua portuguesa ou inglesa, devendo ter-se em conta que:

- 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.
- 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.
- Todas as peças devem conter: bloco de assinaturas; controlo de versões, controlo de cópias e índice.
- O bloco de assinaturas deve conter: a assinatura de quem preparou (CISP/CISOA), de quem aprovou (CISOA/CISPIA) e de quem vai autorizar (SAA).
- 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.
- 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.
- Tendo em conta a diversidade de documentação requerida, o detalhe que diz respeito a cada documento encontra-se no Anexo D da NT - B01.

POSSO UTILIZAR UM SISTEMA NÃO ACREDITADO PARA MANUSEAR INFORMAÇÃO CLASSIFICADA?

Não. Apenas os sistemas acreditados pela ANS podem manusear informação classificada.

TENHO UM SISTEMA QUE PROCESSA INFORMAÇÃO ATÉ RESERVADO DEVO PROCEDER À SUA ACREDITAÇÃO DE SEGURANÇA?

Sim. Apesar dos requisitos para manusear informação de grau RESERVADO serem de uma forma geral mais ligeiros, este requer uma autorização formal da ANS e como tal deve ter um processo de acreditação de segurança que distingue o sistema em causa dos demais sistemas de informação e comunicação da organização.

O QUE É PRECISO PARA INTERLIGAR/INTERCONECTAR UM SISTEMA ACREDITADO A UM OUTRO SISTEMA?

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 ao GNS.
Para estabelecer uma interligação devem ser desenvolvidas as seguintes atividades;

- Atividade I-01 – Justificação da Interligação (SISRS);
- Atividade I-02 – Avaliação do Risco da Interligação;
- Atividade I-03 – Revisão de SSRS e Secops;
- Atividade I-04 – Decisão sobre a acreditação de segurança da interligação.

POSSO INTERLIGAR UM SISTEMA NÃO ACREDITADO A UM SISTEMA ACREDITADO?

Não. Apenas sistemas acreditados pela ANS podem ser interligados.

POSSO INTERLIGAR UM SISTEMA ACREDITADO COM A INTERNET?

Sim é possível para alguns graus, mas existem regras específicas para o estabelecimento de conectividade com a internet.

TENHO UMA EMPRESA E PRECISO TRATAR INFORMAÇÃO CLASSIFICADA, PRECISO ACREDITAR O MEU POSTO DE TRABALHO?

Sim. Apenas sistemas acreditados pela ANS podem tratar informação classificada.

PRECISO RESPONDER A UM CONTRATO CLASSIFICADO, PRECISO TER UM POSTO DE TRABALHO ACREDITADO?

Sim. Apenas sistemas acreditados pela ANS podem tratar informação classificada.

TENHO UMA EMPRESA E QUERO INFORMATIZAR O NOSSO POSTO DE CONTROLO, O QUE PRECISO PARA ACREDITAR O MEU POSTO DE TRABALHO?

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.

O processo de acreditação de um SIC pertencentes a entidades privadas, vulgo empresas, pode assumir a tipologia: Offline ou Online.
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, conforme anexo F à NT-B01.

O processo de acreditação de um SIC para operação em modo Online, segue o processo de acreditação descrito no ponto 11 da NT-B01.

Qualquer que seja o processo de acreditação conduzido para o SIC, é necessário realizar uma avaliação de segurança física e eletrónica, assim como, uma auditoria de segurança aos equipamentos que irão ser utilizados para manusear informação classificada.

Salienta-se ainda que o processo de 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.