CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

ESQUEMA DE CERTIFICAÇÃO DE SERVIÇOS DE CIBERSEGURANÇA

Índice

1. Objeto e âmbito de aplicação

O Centro Nacional de Cibersegurança (CNCS), enquanto Autoridade Nacional de Certificação da Cibersegurança (ANCC), tem vindo a desenvolver um quadro nacional de certificação da cibersegurança.

O presente documento vem concretizar a criação de um esquema de certificação de serviços de cibersegurança, no âmbito da competência de desenvolvimento e implementação de esquemas nacionais específicos de certificação da cibersegurança atribuída à ANCC, conforme previsto no Art.º20 do Decreto-Lei n. º 65/2021.

O Esquema de Certificação de Serviços de Cibersegurança (EC SCS) é o segundo esquema do quadro nacional de certificação da cibersegurança, promovido pelo CNCS enquanto ANCC, após a publicação do esquema de certificação da conformidade com o Quadro Nacional de Referência para a Cibersegurança (EC QNRCS), em dezembro de 2022.

O presente EC SCS é de carácter voluntário e aplica-se a todas as organizações que prestam serviços de cibersegurança, de todas as tipologias e dimensões e que estejam estabelecidas em território nacional.

O âmbito de aplicação da certificação no presente esquema é a implementação dos requisitos de segurança especificados nos vários anexos do presente esquema, dentro de uma determinada tipologia de serviço prestado.

Caso se trate de uma organização plurilocal, o âmbito da certificação deve incluir a prestação do serviço em causa, independentemente do local.

2. Objetivo do Esquema de Certificação de Serviços de Cibersegurança

A certificação neste novo esquema procura responder à necessidade da identificação e valorização de serviços de cibersegurança cujo desempenho passa a ser alvo de avaliação e monitorização periódica, apoiando a elaboração de um catálogo de prestadores de serviços de cibersegurança nacionais confiáveis, que atendam à procura existente quer a nível nacional como internacional, elevando a reputação das organizações nacionais e facilitando a sua integração no mercado europeu e ou internacional de prestação de serviços de cibersegurança.

O presente documento vem especificar os requisitos para a certificação acreditada das organizações que pretendem demonstrar a sua conformidade com os requisitos gerais, aplicáveis a todas as organizações, que prestem serviços de cibersegurança das tipologias abrangidas e com os requisitos e especificidades técnicas próprias definidos para cada tipo de serviço de cibersegurança prestado.

No âmbito deste documento foram definidos os seguintes serviços de cibersegurança:

- Anexo 2.1 - Monitorização e resposta a incidentes;
- Anexo 2.2 - Gestão de vulnerabilidades;
- Anexo 2.3 - Informações sobre ameaças *(Threat Intelligence)*;
- Anexo 2.4 - Teste de Intrusão.

3. Uso de normas de referência

O EC SCS está definido em função dos requisitos e orientações estabelecidas nos diplomas legais nacionais e europeus aplicáveis, em normas e referenciais de boas práticas disponibilizados pelo CNCS, e ainda em fontes internacionalmente reconhecidas:

- Os elementos constituintes do EC SCS regem-se, com as necessárias adaptações, pelas disposições constantes do título III do Regulamento (UE) 2019/881, seguindo, em particular, tanto quanto possível e aplicável, os elementos definidos no art.º 54 daquele normativo; por conseguinte, a estrutura e conteúdos dos esquemas europeus *EU Common Criteria Scheme* (EUCC) e *EU Cloud Services Scheme (*EUCS) também serviram de inspiração para o EC SCS;
- Enquanto segundo esquema do quadro nacional de certificação em cibersegurança, promovido pelo CNCS enquanto ANCC, o presente esquema de certificação está alinhado com a estrutura, orientações e conceitos presentes no Esquema de Certificação Quadro Nacional de Referência para a Cibersegurança (EC QNRCS);
- Uma outra fonte de inspiração do presente esquema foi a estrutura do esquema de certificação contido no DNP TS 4577-1 Maturidade digital – Selo digital, Parte 1: Cibersegurança, parcialmente desenvolvido pelo CNCS;
- A terminologia utilizada no EC SCS tem por referência a terminologia e definições da ISO/IEC 27001, EN ISO 19011 e NIST *Cybersecurity Framework*;
- A norma ISO/IEC 17065 é a norma internacional para a acreditação dos organismos de avaliação de conformidade no âmbito do EC SCS;
- Os requisitos de implementação de medidas para fins de certificação no âmbito do presente esquema, bem como as evidências de verificação associadas, estão definidos nos Anexos 1 e 2 do presente esquema;
- O presente esquema reconhece os requisitos existentes na ISO/IEC 27001 e no EC QNRSC, promovendo a sua adoção de forma a potenciar o aumento da resiliência e segurança das organizações que prestam serviços de cibersegurança, contribuindo de forma decisiva para a confiança do mercado nestes prestadores de serviço;

4. Termos e definições

Para os fins do presente documento aplicam-se os seguintes termos e definições:

4.1. Monitorização e resposta a incidentes de segurança

Monitorização de sistemas, aplicações e redes que permita a identificação e resposta eficaz a incidentes de segurança informática, envolvendo a definição de "incidente", estabelecimento de serviços, criação de políticas e procedimentos, e garantia da autonomia da equipa, com foco na integração interna e colaboração externa.

4.2. Gestão de vulnerabilidades

Avaliação sistemática de um sistema ou produto de informação para determinar a eficácia das medidas de segurança, identificar falhas, prever o desempenho de soluções propostas e confirmar sua adequação após a implementação.

4.3. Informações sobre ameaças (Threat Intelligence)

Informações sobre ameaças (Threat Intelligence) refere-se à recolha e tratamento de dados sobre ameaças de segurança em informações processadas e analisadas, que fornecem contexto valioso e acionável para apoiar decisões estratégicas e táticas em Cibersegurança. Este processo permite que as organizações antecipem, identifiquem e respondam proactivamente a ameaças, com base numa compreensão detalhada das técnicas e motivações dos atacantes.

4.4. Teste de intrusão

Método de teste que avalia a segurança de sistemas, redes e aplicações para identificar vulnerabilidades que possam ser exploradas para comprometer a segurança.

4.5. Gestão do risco

A gestão dos riscos é o processo sistemático de identificar, avaliar e tratar riscos que possam afetar a confidencialidade, integridade e disponibilidade de informações numa organização. Este processo envolve a análise contínua de potenciais ameaças, a avaliação da probabilidade e impacto dessas ameaças, e a implementação de controlos e medidas de mitigação para reduzir os riscos a níveis aceitáveis. Uma gestão eficaz dos riscos é essencial para garantir que as operações de uma organização possam continuar de forma segura e resiliente, mesmo face a incertezas e ameaças cibernéticas.

4.6. Auditoria interna

Processo sistemático independente e documentado para obter evidência objetiva e respetiva avaliação objetiva com vista a determinar os critérios de auditoria.

4.7. Organização

Entidade com personalidade jurídica, prestadora de serviços de cibersegurança, estabelecida em território nacional. Realiza atividades económicas com finalidades comerciais, por meio da produção e venda de bens ou serviços.

NOTA 1 à secção: O conceito de organização inclui, mas não se limita a companhia, corporação, firma, empresa, dotadas de personalidade jurídica, de direito público ou privado.

4.8. Local

Instalação, na dependência da função central, onde são desenvolvidos processos e atividades controladas, monitorizadas e medidas pela função central.

4.9. Função central

Parte da organização responsável pela definição, planeamento e controlo dos processos e procedimentos relevantes para o âmbito da certificação.

4.10. Organização plurilocal

Organização (4.7) que dispõe de uma função central (4.9) com mais do que um local (4.8).

4.11. Processo

Conjunto de atividades interrelacionadas ou interatuantes que transformam entradas em saídas.

4.12. Procedimento

Modo especificado de realizar uma atividade ou um processo (4.11).

NOTA 1 à secção: Os procedimentos poderão ser documentados ou não.

4.13. Auditoria de certificação

Processo (4.11) sistemático, independente e documentado para obter evidência objetiva e respetiva avaliação objetiva com vista a determinar em que medida os requisitos das normas de certificação estão a ser cumpridos.

4.14. Conformidade

Satisfação de um requisito.

4.15. Não conformidade

Não satisfação de um requisito.

4.16. Ação corretiva

Ação para eliminar a causa de uma não conformidade (4.15) para prevenir a sua recorrência.

4.17. Correção

Ação para eliminar uma não conformidade (4.15) detetada.

NOTA 1 à secção: Uma correção pode ser efetuada antes de, em conjunto com ou depois de uma ação corretiva (4.16).

4.18. Requisito

Necessidade ou expetativa expressa, geralmente implícita ou obrigatória.

NOTA 1 à secção: «Geralmente implícita» significa que é hábito ou prática comum para a organização (4.7) e para as partes interessadas que a necessidade ou expetativa em consideração esteja implícita.

NOTA 2 à secção: Um requisito especificado é um requisito que é expresso, p. ex. em informação documentada.

5. Requisitos gerais e requisitos específicos

O EC SCS estabelece requisitos gerais horizontais aplicáveis a todas as organizações candidatas, independentemente do serviço que prestem, e também estabelece requisitos específicos obrigatórios por tipo de serviço que os prestadores de cibersegurança devem implementar e cumprir aquando da prestação dos seus serviços para efeitos da obtenção da certificação.

Uma organização candidata à certificação deve cumprir os requisitos gerais contidos no Anexo 1 do presente esquema de certificação, bem como os requisitos específicos de cada serviço a que se candidata, estabelecidos nos anexos 2.1 a 2.4.

6. Níveis de certificação

São definidos dois níveis de certificação, de modo que as organizações possam selecionar o nível mais adequado em função da sua realidade e estratégia definida de acordo com os seus clientes e/ou potenciais clientes.

A diferenciação entre os dois níveis de certificação, básico e substancial, faz-se pela Credenciação de Segurança do prestador de serviços de cibersegurança, requerida ao Gabinete Nacional de Segurança. No nível substancial as organizações, para além dos requisitos gerais e requisitos mínimos específicos por tipo de serviço, devem possuir a Credenciação de Segurança, aplicável à organização e a todas as pessoas envolvidas na prestação dos serviços de cibersegurança no âmbito da certificação, incluindo subcontratados.

7. Requisitos para implementação

No que respeita à estrutura dos requisitos, o presente documento define um conjunto de requisitos de segurança distribuídos por três categorias distintas – organizacional, humana e técnica – que a organização candidata à certificação deve implementar, assim como os métodos e procedimentos de verificação de tal implementação. Estes encontram-se descritos numa linguagem clara, que permite às organizações, intuitivamente, apreender o que delas é esperado e como devem cumprir com os requisitos.

O presente documento pretende ainda orientar os organismos de certificação (OC) nos procedimentos a aplicar para verificação da conformidade com os requisitos.

Os requisitos para a certificação e evidências de auditoria para a decisão de certificação estão definidos nos Anexos 1 e 2.

Os requisitos definidos são todos de carácter obrigatório e estão organizados em 3 categorias:

- Organizacional: inclui requisitos relacionados com a estrutura, funções e políticas de cibersegurança;
- Técnica: inclui os requisitos relacionados com as medidas técnicas e tecnológicas;
- Humana: inclui os requisitos relacionados com as competências do pessoal.

8. Métodos e critérios de avaliação

A conformidade de uma organização candidata à certificação de serviços de cibersegurança, resulta da decisão do Organismo de Certificação (OC), em função dos resultados obtidos na auditoria de certificação. Esta decisão deve resultar da(s) auditoria(s) realizada(s) e da respetiva resposta ao resultado da(s) auditoria(s) pela organização candidata.

Os ciclos de certificação são de 3 anos, organizados da seguinte forma: uma auditoria de concessão, 2 auditorias de acompanhamento e uma auditoria de renovação. Após a auditoria de renovação, repetem-se as 2 auditorias de acompanhamento e assim sucessivamente.

A função central deve assegurar o cumprimento de todos os requisitos gerais e específicos do serviço prestado caso seja uma organização plurilocal e deve ainda assegurar que todas as evidências associadas ao cumprimento dos requisitos são auditáveis a partir da função central.

Nas auditorias de concessão e de renovação deve ser verificada a implementação de todos os requisitos, e devidas evidências, devendo haver especial atenção para o facto dos requisitos gerais identificados no Anexo 1 do esquema de certificação de serviços de cibersegurança serem de cumprimento e avaliação obrigatória para todos os serviços de cibersegurança no âmbito deste EC.

Nas auditorias de acompanhamento anuais, o OC deve selecionar quais os requisitos a avaliar entre a primeira e a segunda auditoria anual, sendo que no cômputo de ambas devem ser verificados todos os requisitos definidos para o(s) serviço(s) e respetivo nível de certificação. As evidências de conformidade que a organização candidata deve apresentar encontram-se identificadas para todos os requisitos obrigatórios, gerais e por serviço, e devem ser confirmadas pelo OC no decurso da(s) auditoria(s), sendo que poderão ser solicitadas evidências adicionais em função das características específicas dos serviços, sistemas, recursos, processos e procedimentos da organização.

Compete ao OC a análise do conjunto de evidências recolhidas e a produção de constatações de conformidade sustentadas, em cada requisito analisado. No entanto, da análise de cada requisito, para além da conformidade, podem resultar outras constatações referidas abaixo:

- Não conformidade Maior – Ocorre nos casos em que o requisito não se encontra implementado ou, se implementado, encontra-se totalmente desalinhado dos seus objetivos;
- Não conformidade Menor – Ocorre nos casos em que o requisito se encontra implementado, mas não consegue demonstrar totalmente que cumpre os respetivos objetivos;
- Oportunidade de Melhoria – Ocorre nos casos em que o requisito se encontra implementado, consegue demonstrar a obtenção dos respetivos objetivos, mas não o está a fazer da forma mais eficaz. Poderá ainda ser associada a situações em que a oportunidade de melhoria possa prevenir futuras não conformidades.

Tanto as não conformidades (Maior ou Menor) como as oportunidades de melhoria, devem ser registadas e devidamente enquadradas no Relatório de Auditoria, produzido pelo OC e entregue à organização auditada.

8.1. Regras para o tratamento de "Não conformidades"

As diligências para resolução de não conformidades devem seguir o seguinte encadeamento:

1. O OC informa a organização candidata sobre as não conformidades detetadas, identificando-as, e solicita a entrega de um Plano de Ações Corretivas (PAC)
2. Entrega ao OC do PAC pela organização candidata
3. Avaliação do PAC pelo OC:

- Se o PAC for aceite, é concedido um prazo para a organização candidata implementar as correções e/ou ações corretivas indicadas no PAC, dentro dos prazos e moldes previstos mais abaixo
- Se o PAC contiver correções e/ou ações corretivas para encerramento de não conformidades maiores e não for aceite pelo OC, este declara parecer negativo para certificação e o processo termina

4. No caso de se estarem a tratar não conformidades maiores, por princípio, o OC deve desencadear a realização de auditoria de seguimento para o seu encerramento, excetuando-se nas situações em que é possível avaliar a adequabilidade e implementação das ações e a sua eficácia de forma documental.

Para encerrar as não conformidades, a organização candidata deve proceder à criação e entrega ao OC, no prazo máximo de 30 dias de calendário desde a apresentação da Não Conformidade, de um PAC onde estabelece as ações a implementar, responsáveis e prazos de implementação. O OC deve analisar a proposta de PAC, informando a organização candidata da sua aprovação ou não aprovação, no prazo máximo de 10 dias úteis. Para encerramento de Não conformidades Maiores, e após aprovação do PAC pelo OC, a organização candidata deve apresentar as evidências de implementação dentro de um prazo máximo de 30 dias de calendário desde a apresentação da Não Conformidade.

Para encerramento das Não conformidades menores, a organização deverá produzir e enviar um PAC ao OC, implementando as ações nele constantes o mais rapidamente possível dentro de um prazo não superior a 60 dias de calendário desde a apresentação da Não Conformidade. As evidências de implementação serão obrigatoriamente verificadas na próxima auditoria de acompanhamento.

O certificado só será emitido com todas as evidências de implementação das ações relativas às Não conformidades Maiores aceites pelo OC, e com o PAC aprovado pelo OC no caso de lhe terem sido identificadas Não conformidades menores.

9. Requisitos para a candidatura à certificação EC SCS

As organizações candidatas à certificação no EC SCS devem:

- estar legalmente constituídas e estabelecidas em território nacional, possuindo uma personalidade jurídica própria e disponibilizando a certidão permanente de registo comercial;
- corresponder a uma única entidade legal;
- estar em situação de cumprimento para com as obrigações legais que sobre si impendem, especialmente as de cibersegurança, e, sobretudo, caso se trate de uma entidade abrangida pelo Regime Jurídico da Segurança do Ciberespaço;
- eleger o nível de certificação a que se querem candidatar;
- possuir evidência de certificado ou instrução do processo de certificação, no âmbito dos serviços a prestar, num dos seguintes referenciais:
    - ISO 27001 (última versão)– *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*
    - EC QNRCS (última versão) – Esquema de Certificação no Quadro nacional de Referência em Cibersegurança;
    - De notar que uma decisão de certificação favorável no âmbito do presente esquema de certificação, apenas é possível após evidência de certificado válido num dos dois referenciais anteriormente referidos;
- ter implementados, para o(s) serviço(s) a que se candidatam, todos os requisitos aplicáveis, gerais e específicos por serviço:
- caso a organização se candidate a uma certificação de nível substancial deve demonstrar que a organização e todas as pessoas envolvidas na prestação dos serviços de cibersegurança no âmbito da certificação, incluindo subcontratados possuem Credenciação de Segurança;
- ter registadas as evidências da implementação dos requisitos obrigatórios, gerais e específicos por serviço selecionada para a certificação; disponibilizar e garantir a veracidade das informações e os contactos solicitados no formulário de candidatura, que deverá ser entregue a um OC;
- comprometer-se a comunicar ao OC, imediatamente e sem demora injustificada, no prazo máximo de 5 dias úteis, qualquer incidente de cibersegurança e segurança da informação que provoque impactos no que respeite à confidencialidade, integridade e disponibilidade da segurança da informação,

das redes, dos sistemas de informação abrangidos no âmbito de certificação SCS da organização e que, por isso, afete a validade do certificado;

- comprometer-se a comunicar ao OC, imediatamente e sem demora injustificada, no prazo máximo de 5 dias úteis, qualquer suspensão ou anulação de certificação e respetivas causas da ISO 27001 ou do EC QNRCS, que possa ocorrer e que ponha em causa o cumprimento dos requisitos do EC SCS;
- comprometer-se a comunicar ao OC, imediatamente e sem demora injustificada, no prazo máximo de 5 dias úteis, qualquer alteração de âmbito na certificação ISO 27001 ou no EC QNRCS;
- comprometer-se a comunicar ao OC, imediatamente e sem demora injustificada, no prazo máximo de 5 dias úteis, qualquer alteração no âmbito dos serviços prestados que tenha impacto ou possa comprometer a atividade desenvolvida no âmbito da certificação.

Os requisitos para os candidatos à certificação do EC SCS devem ser analisados pelos OC, após a receção do respetivo formulário de candidatura à certificação SCS.

10. Marcas e rótulos

A definir

11. Processo de certificação e gestão de certificados

O processo de certificação do EC SCS está estruturado com base em 4 atores e/ou categorias de atores principais e correspondentes papeis:

- CNCS – Centro Nacional de Cibersegurança;
- IPAC – Instituto Português de Acreditação;
- OC – Organismos de Certificação;
- Organizações prestadoras de serviços de cibersegurança candidatas.

Os papéis, funções e responsabilidades de cada um destes atores no EC SCS são apresentados na tabela seguinte:

Entidades(s) / Siglas	Papéis	Funções e Responsabilidades
IPAC	Organismo Nacional de Acreditação	• Prestar serviços de acreditação aos OC para execução do processo de certificação do EC SCS • Tratar reclamações sobre os OC em articulação com o CNCS se necessário • Articular com o CNCS o processo de supervisão • Elaborar e publicar o esquema de acreditação dos OC para fins de certificação no EC SCS
CNCS	Autoridade Nacional de Certificação em Cibersegurança	• Elaborar, gerir, manter, atualizar e publicitar o Esquema de Certificação SCS • Supervisionar os certificados emitidos e as organizações certificadas • Apoiar o IPAC na supervisão dos OC • Apoiar o IPAC na elaboração do esquema de acreditação dos OC para fins de certificação no EC SCS • Emitir os códigos QR a constar nos certificados • Gerir a página web para publicação dos certificados SCS • Estabelecer-se como ponto de contacto para a cooperação internacional no plano da certificação europeia em cibersegurança
OC	Organismos de Certificação	• Obter e manter a acreditação pelo IPAC, de acordo com a EN/ISO 17065 • Receber e validar as candidaturas à certificação no EC SCS • Executar o processo de certificação SCS • Proferir a decisão de certificação SCS

		• Emitir os certificados SCS e gerir os respetivos ciclos de vida • Cumprir e fazer cumprir as regras e requisitos do EC SCS, incluindo a Política de divulgação dos certificados SCS
Organizações candidatas	Organizações prestadoras de serviços de cibersegurança candidatas à certificação SCS	• Cumprir com as obrigações legais a que está sujeita, em especial as alusivas à sua situação de cibersegurança no âmbito dos serviços a prestar • Implementar todos os requisitos previstos no EC SCS • Executar a candidatura a um nível de certificação SCS • Disponibilizar evidências da implementação dos requisitos de EC SCS • Cumprir as regras e requisitos do EC SCS, incluindo a Política de divulgação dos certificados SCS

11.1. Requisitos para os Organismos de Certificação

É obrigação dos OC observar as seguintes regras gerais do EC SCS:

- tratar a informação recebida das organizações candidatas com confidencialidade, assegurando o respetivo tratamento interno no estrito cumprimento das práticas de gestão da segurança da informação associada, nomeadamente em termos de controlo de acessos e de partilha com terceiras partes;
- cumprir os procedimentos de comunicação com o CNCS estabelecidos no âmbito do EC SCS;
- cumprir com todos os demais requisitos definidos no EC SCS para os OC, incluindo a Política de divulgação dos certificados SCS;
- participar nas atividades de supervisão do EC SCS pelo CNCS, sempre que solicitados nos casos aplicáveis.
- investigar e atuar diligentemente sobre situações de não conformidade detetadas em certificados por si emitidos, ou de incumprimento de regras do EC SCS por parte de organizações por si certificadas, comunicadas pelo CNCS ou por qualquer outra via chegadas ao seu conhecimento, tendo em vista o rápido restabelecimento da situação de conformidade dos certificados ou de cumprimento dos demais requisitos do esquema. Os requisitos e regras a que os organismos de certificação estão assim sujeitos procuram garantir a sua

qualificação e proficiência nas normas e procedimentos estabelecidos e amplamente reconhecidos em matérias de certificação e de cibersegurança, bem como a sua idoneidade, isenção e imparcialidade na condução dos processos de certificação. Como consequência, os certificados por estes emitidos beneficiam de credibilidade e de legitimidade nos mais diversos contextos de utilização, inclusive internacionais.

- Avaliar o pedido de equivalência apresentado pela organização prestadora do serviço de cibersegurança, relativamente à certificação da Equipa afeta à prestação do serviço. Sempre que neste processo de avaliação de equivalência seja identificado pelo OC uma nova certificação equivalente aplicável, o OC submete à apreciação do CNCS a aceitação e posterior inclusão de uma nova certificação na lista de certificações equivalentes. Caso o CNCS aprove esta inclusão, procede à atualização da lista de certificações equivalentes no site do CNCS.

11.2. Ciclo de vida

11.2.1. Validade dos certificados

O período de validade dos certificados de conformidade com o EC SCS é de três anos após a emissão, salvo motivo superveniente que conduza à sua anulação antes daquele prazo.

11.2.2. Manutenção da certificação

A manutenção da validade do certificado requer a realização de uma auditoria de acompanhamento transcorrido cada ano, ou seja, deverá ser efetuada uma primeira auditoria de acompanhamento passado um ano da auditoria de concessão e uma segunda auditoria de acompanhamento passados dois anos.

Compete ao OC agendar as auditorias, tendo em atenção os prazos abaixo estipulados e a organização certificada deverá cooperar no sentido de se manter disponível e assegurar o bom curso das auditorias.

11.2.3. Renovação da certificação

O ciclo de certificação renova-se ao terceiro ano, por meio de uma auditoria de renovação, à qual são aplicáveis os requisitos acima descritos.

11.3. Processo de certificação

O processo de certificação do EC SCS pode-se resumir através do seguinte encadeamento de etapas e prazos associados:

1. Candidatura da organização à certificação do EC SCS junto do OC
2. Análise e validação da candidatura pelo OC:
   - o OC tem um prazo de 15 dias úteis para confirmar, ou não, a aceitação de uma candidatura;
3. Realização da auditoria de concessão pelo OC:
   - deve ser iniciada num prazo previamente acordado entre as partes, mas que não deve ultrapassar 90 dias de calendário;
   - é verificada a implementação dos requisitos requeridos, considerando o nível de certificação manifestado na candidatura, através dos critérios e evidências definidos, gerais e específicos por serviço a que a organização se candidata;
   - caso sejam detetadas não conformidades, dever-se-ão encetar os passos detalhados no Capítulo 8.1 - Regras para o tratamento de “Não conformidades”
4. Análise e revisão do relatório de auditoria e das evidências apuradas por parte do OC
5. Decisão de certificação pelo OC:
   - quando demonstrada a conformidade em todos os requisitos, gerais e associados ao(s) serviço(s) a certificar, no nível de certificação selecionado;
6. Emissão de certificado pelo OC;
   - com um período de validade de 3 anos;
7. Publicação dos certificados do EC SCS de acordo com o referido na Política de divulgação dos certificados do EC SCS;
8. Realização da auditoria de acompanhamento anual:
   - deve ter uma variação máxima de 30 dias de calendário em relação ao mês e finalização da auditoria de concessão;

9. Realização da auditoria de renovação da certificação do EC SCS / início de novo ciclo
   - deve ser realizada até 30 dias de calendário anteriores ao término da data de validade do certificado SCS em vigor;
10. Realização de auditorias extraordinárias:
    - sempre que:
      i. após a certificação, ocorram alterações significativas na organização certificada e que sejam consideradas no âmbito de certificação do EC SCS ou que tenham consequências na definição desse âmbito;
      ii. o OC o determine, para verificação de uma situação de incumprimento chegada ao seu conhecimento;
      iii. determinadas pelo CNCS na sua qualidade de ANCC.

As auditorias extraordinárias são utilizadas quando a organização certificada quer alterar os pressupostos iniciais da certificação (mudança de instalações, fusão, extensão do âmbito, entre outras). Estas auditorias podem ser efetuadas em qualquer momento entre as auditorias planeadas. As auditorias extraordinárias podem ainda ocorrer, por decisão do OC, na sequência de uma notificação pela organização certificada de um incidente de cibersegurança que provoque impactos no que respeita à confidencialidade, integridade e disponibilidade da segurança das redes e dos sistemas de informação abrangidos no âmbito de certificação SCS da organização e que, por isso, afete a validade do certificado, ou ainda na sequência da notificação de suspensão ou anulação da certificação na ISO 27001 ou no EC QNRCS.

11. Realização de auditorias de seguimento:
    - sempre que no seguimento de auditorias prévias de concessão, de renovação ou de acompanhamento, para a confirmação da execução com eficácia de um Plano de Ações Corretivas;
11. Revogação de certificados do EC SCS pelos OC:
    - no caso de não cumprimento pelas organizações candidatas das regras definidas pelo EC SCS;
    - a decisão de revogação deve ser comunicada à organização certificada e ao CNCS no prazo máximo de 5 dias úteis

11.4. Estados dos certificados

Os certificados do EC SCS emitidos pelo OC podem estar associados aos seguintes estados:

- **Atribuído** – quando da decisão positiva de certificação da conformidade com o EC SCS pelo OC;
- **Suspenso** – pode ocorrer a necessidade de suspensão de um certificado do EC SCS, pelo menos nas seguintes circunstâncias, entre outras:
    - Execução não eficaz de um Plano de Ações Corretivas da organização certificada;
    - Identificação de não conformidades associadas ao certificado ou de incumprimentos das regras do EC SCS por parte da organização certificada, através da comunicação pelo CNCS ao OC das irregularidades detetadas durante as atividades de supervisão do EC SCS, ou por qualquer outra via chegadas ao seu conhecimento;
    - Quando existe a suspensão da certificação na ISO 27001 ou no EC QNRCS.

O prazo de suspensão de um certificado do EC SCS não pode ultrapassar 6 meses.

A suspensão da certificação deve ser levantada quando se demonstrar que a causa que esteve na origem da suspensão da certificação já não existe. O levantamento da suspensão da certificação pode ser feito através da análise de evidências documentais, quando suficiente, ou através de auditorias que não substituem as auditorias previstas do ciclo de certificação.

Durante o período de suspensão da certificação, a entidade certificada não pode fazer qualquer referência ao estatuto de entidade certificada e fica impossibilitada de utilizar a marca de certificação.

Após o levantamento da suspensão, o ciclo de certificação é retomado, mantendo-se a data de validade original do certificado de conformidade, não havendo lugar a qualquer prorrogação do seu prazo de validade.

- **Revogado** – quando o OC identifica ou é informado de situações de não cumprimento do EC SCS por parte da organização certificada, inclusive através de comunicação pelo CNCS no seguimento das suas atividades de supervisão do EC SCS, e designadamente nos casos em que, estando o

certificado suspenso, não há pela organização certificada a observância do disposto pelo OC para restabelecimento da conformidade e levantamento da suspensão. É ainda aplicada nas situações de encerramento da organização (falência ou deslocação para outra zona geográfica), e/ou no caso de compra por, ou fusão com outra organização não certificada. Neste caso, a organização não pode fazer qualquer referência ao estatuto de entidade certificada, bem como não pode fazer qualquer utilização do certificado de conformidade e da marca e/ou rótulo de certificação.

- **Expirado** – quando o certificado do EC SCS atingiu o final do seu prazo de validade.

11.5. Transferência

O EC SCS admite a transferência da certificação entre OC pela organização certificada mediante as seguintes condições:

- o certificado estar dentro de prazo de validade;
- ambos os OC envolvidos no procedimento de transferência devem estar devidamente acreditados para este esquema.

Deve ser solicitado ao OC que originalmente emitiu o certificado uma declaração em como as auditorias do presente ciclo se encontram todas realizadas e as não conformidades encerradas, e de que não existem incidências pendentes com a organização a transferir (por exemplo, reclamações ou dívidas).

O OC que emitiu originalmente o certificado não poderá anular o certificado antes de todas as atividades de transferência estarem concluídas.

Na eventualidade do certificado atingir o termo da validade durante as atividades de transferência, o certificado a emitir pelo novo OC apresentará um intervalo entre a data de validade do certificado anterior e a data de emissão do novo.

A auditoria de transferência deve ser efetuada antes do termo de validade do certificado.

A transferência pode ser efetuada em qualquer altura do ciclo de certificação, no entanto a auditoria de transferência deve ser equiparada a uma auditoria de recertificação, para que o novo OC e a respetiva equipa auditora possam fazer uma análise adequada da documentação e das práticas da organização transferida.

A auditoria de transferência inclui a análise dos relatórios do ciclo anterior e o teor das não conformidades das auditorias, de modo a identificar e avaliar recorrências.

A auditoria decorrerá de acordo com o estipulado para as restantes auditorias.

O novo certificado deve dar continuidade à validade do certificado do OC anterior, com um prazo de validade de 3 anos.

11.6. Anulação Voluntária

A qualquer altura do ciclo de certificação a organização poderá pedir a anulação do seu certificado, enviando um pedido para o OC, que comunicará essa decisão ao CNCS.

12. Regras referentes a incumprimentos

Em cumprimento do disposto pelo Art.º 21º do Decreto-Lei n.º 65/2021, a organização certificada estará sujeita a sanções no caso de incorrer nas infrações nele previstas, sendo o CNCS, na qualidade de ANCC, a entidade responsável pela sua aplicação.

13. Conteúdo e formato do certificado

A definir

14. Política de divulgação dos certificados

A definir

15. Referências

A definir

Lista de Requisitos EC SCS

Requisitos Gerais - RG

Referência	Requisito	Definição	Categoria	Evidências
RG.01	**Risco decorrente da atividade**	A Organização deve ter disposições adequadas (por exemplo seguros e fundos de reserva) para cobrir as responsabilidades decorrentes da sua atividade.	Organizacionais	**A organização deve evidenciar as medidas adotadas, nomeadamente: - disponibilizar o número da apólice de seguro e respetivas condições gerais e particulares; - demonstração financeira e relatório de gestão.**
RG.02	**Gestão dos Riscos**	A organização deve elaborar um Plano de Gestão do Risco que identifique cenários que possam provocar exposição indevida de informação, interrupção ou alteração no(s) sistema(s), rede(s), aplicação(ões), ou outro com impacto negativo no cliente durante ou decorrente da prestação do serviço. Deve também identificar as ações a implementar para mitigar os riscos identificados. Este plano deve ser formalmente aprovado pelo cliente.	Organizacionais	**A organização deve disponibilizar o Plano de Gestão do Risco, devidamente aprovado pelo cliente. Deve também evidenciar a implementação das medidas de mitigação constantes do Plano de Gestão de Risco.**
RG.03	**Vínculo contratual do pessoal afeto à realização dos serviços**	A organização deve evidenciar a existência de um vínculo contratual entre a mesma e as pessoas da organização, internas ou externas, que possam influenciar as atividades no âmbito da certificação. O contrato pode ser a tempo integral ou parcial, contituir regime de trabalho por conta de outrem ou prestação de serviço.	Organizacionais	**A organização deve disponibilizar o vinculo contratual das pessoas da organização, internas ou externas, que possam influenciar as atividades no âmbito da certificação.**
RG.04	**Autorização para utilização de subcontratados**	A organização deve, no caso de recurso a subcontratado para a prestação do serviço, no âmbito da certificação, obter a autorização formal do cliente. A organização deve ter um contrato com validade jurídica com o subcontratado incluindo disposições para salvaguarda da confidencialidade e do conflito de interesses. A organização deve assumir a responsabilidade por todas as atividades realizadas pelo subcontratado.	Organizacionais	**A organização deve evidenciar: - a autorização dada pelo cliente; - contrato com o subcontratado.**
RG.05	**Código de ética e conduta**	A organização deve dispôr de um código de ética e conduta, devidamente aprovado pela sua gestão de topo e comunicado a todas as pessoas, internas, ou externas, que possam influenciar as atividades no âmbito da certificação, que inclua pelo menos as seguintes disposições: - todas as atividades são realizadas com lealdade, discrição e imparcialidade; - são utilizados apenas métodos, ferramentas e técnicas devidamente validados e aprovados pela organização; - em todas as atividades realizadas aplica-se a obrigatoriedade de sigilio, confidencialidade e não divulgação, salvo autorização formal por escrito; - compromisso de respeito pela legislação e regulamentação aplicável; - qualquer conflito de interesse entre o colaborador e o cliente deve ser imediatamente comunicado; O código de ética e conduta deve ser revisto em intervalos planeados.	Organizacionais	**A organização deve evidenciar: - o código de ética e conduta devidamente aprovado pela gestão de topo e comunicado a todas as pessoas da organização, internas ou externas, que possam influenciar as atividades no âmbito da certificação; - a revisão do código de ética e conduta;**
RG.06	**Acordo de Confidencialidade**	Deve existir um acordo de confidencialidade assinado pela organização e pelo cliente, de forma a garantir que todas as informações de cliente são protegidas.	Organizacionais	**A organização deve evidenciar o acordo de confidencialidade com o cliente, devidamente assinado pelas duas partes.**
RG.07	**Procedimento disciplinar**	A organização deve dispor de um procedimento formal, a ser acionado sempre que pessoas, internas ou externas à organização, que possam influenciar as atividades no âmbito da certificação, não cumpram o código de conduta e ética em vigor na organização. Este procedimento deve ser comunicado a todas as pessoas, internas ou externas à organização, que possam influenciar as atividades no âmbito da certificação.	Organizacionais	**A organização deve evidenciar: - a comunicação da existência de procedimento disciplinar a todas as pessoas da organização, internas ou externas, que possam influenciar as atividades no âmbito da certificação. ; - o registo de qualquer procedimento disciplinar levado a cabo na organização;**

Referência	Requisito	Definição	Categoria	Evidências
RG.08	**Acompanhamento pelo cliente**	A organização deve definir um plano para comunicações seguras e regulares, mecanismos de feedback e um processo claro para atualizar o cliente sobre a prestação do serviço.	Organizacionais	**A organização deve apresentar evidências do desenvolvimento e a implementação de um plano de envolvimento do cliente que inclua comunicações regulares e seguras e mecanismos de feedback para garantir a colaboração e a confiança.**
RG.09	**Tratamento de reclamações**	A organização deve dispor de um procedimento documentado para análise, tratamento e comunicação das conclusões ao cliente, relativo às reclamações recebidas no âmbito da certificação.	Organizacionais	**A organização deve evidenciar registos de tratamento das reclamações recebidas, no âmbito da certificação e respetivas respostas ao cliente.**

Monitorização e Resposta a Incidentes – MR

Referência	Requisito	Definição	Categoria	Evidências
MR.01	**Proposta**	A organização deve manter registos de proposta para a execução do serviço de monitorização e resposta a incidente, a qual deve incluir no mínimo, a seguinte informação: - âmbito: especificar claramente qual(ais) sistema(s), rede(s), aplicação(ões) a ser(em) incluído(s) na prestação do serviço; - objetivo: identificar o objetivo do serviço; - Duração da prestação do serviço: identificar a duração da prestação do serviço (data de início e témino) e o regime horário da mesma (exemplo: em dias úteis das 9h00 às 18h00 ou 24h/7 dias); - Responsabilidades: identificar a equipa da organização e a equipa interna do cliente e as responsabilidades no âmbito da proposta; - Limitações e restrições: especificar qualquer limitação, como por exemplo a nível de horário ; - Autorização formal: a proposta deve explicitar a necessidade de ser formalmente aprovada pelo cliente; - Confidencialidade: incluir disposições sobre a confidencialidade e como os dados recolhidos durante a prestação do serviço serão protegidos e utilizados; - Entregáveis:especificar claramente os entregáveis resultantes da prestação do serviço de monitorização e resposta a incidentes.	Organizacionais	**A organização deve disponibilizar a proposta e respetiva aceitação, se aplicável, pelo cliente para a execução dos serviços de monitorização e resposta a incidentes.**
MR.02	**Estabelecimento de política de monitorização de segurança**	A organização deve elaborar uma política formal que estabeleça os princípios e diretrizes para a monitorização contínua de segurança, devendo a mesma ser específica e aprovada formalmente pela gestão de topo do cliente. A política deve ser revista em intervalos planeados de forma a garantir que a mesma se mantém adequada aos objetivos do cliente.	Organizacionais	**A organização deve evidenciar:** **- Política documentada de monitorização, aprovada pela gestão de topo do cliente;** **- Registos de revisão e atualização periódica da política.**
MR.03	**Identificação de ativos críticos**	A organização deve, manter registos dos ativos monitorizados no âmbito da prestação do serviço.	Organizacionais	**A organização deve evidenciar:** **- Inventário de ativos monitorizados no âmbito da prestação do serviço.**
MR.04	**Parâmetros de monitorização**	A organização deve manter registos dos parâmetros e métricas utilizados para a prestação do serviço de monitorização.	Técnicos	**A organização deve evidenciar:** **- Parâmetros de monitorização;** **- Relatórios de configuração dos parâmetros .**
MR.05	**Ferramentas de monitorização**	A organização deve proceder à operacionalização das ferramentas de monitorização de eventos de segurança em tempo real. Devem ser produzidos relatórios, em intervalos regulares, de acordo com o acordado entre prestador de serviço e o cliente.	Técnicos	**A organização deve evidenciar:** **- Relatórios de operacionalização;** **- Licenças das ferramentas utilizadas no âmbito da prestação do serviço.**
MR.06	**Monitorização de eventos de segurança**	A organização deve manter registos da supervisão contínua dos eventos de segurança que ocorrem nos ativos incluidos na prestação do serviço.	Técnicos	**A organização deve evidenciar:** **- L*ogs* de eventos;** **- Relatórios de análise de eventos.**
MR.07	**Correlações de Eventos**	A organização deve manter registos da correlação efetuada de diferentes eventos e da identificação de padrões de ataque.	Técnicos	**A organização deve evidenciar:** **- Relatórios de correlação de eventos;** **- Configurações de SIEM (Security Information and Event Management).**

Referência	Requisito	Definição	Categoria	Evidências
MR.08	**Monitorização de tráfego de Rede**	A organização deve manter registos da monitorização contínua do tráfego de rede identificação de ameaças potenciais.	Técnicos	**A organização deve evidenciar:** **- Relatórios de análise de tráfego;** **- Os registos de logs se eventos de rede desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);**
MR.09	**Monitorização de acessos e identidades**	A organização deve manter registos da monitorização dos acessos e da atividade dos utilizadores no sistema. O período mínimo de retenção dos registos, deve ser até à próxima auditoria a realizar pelo organismo de certificação	Técnicos	**A organização deve evidenciar:** **- L*ogs* de acessos, quando aplicável;** **- Relatórios de auditoria de identidade.**
MR.10	**Deteção de intrusões**	A organização deve manter registos da utilização de sistemas de detecção de intrusões (IDS/IPS) para identificar e bloquear atividades suspeitas.	Técnicos	**A organização deve evidenciar:** **- Relatórios de IDS/IPS, *logs* de bloqueios desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);**
MR.11	**Estabelecimento de Política de Resposta a Incidentes**	A organização deve assegurar a existência de uma política de resposta a incidentes de segurança, devendo a mesma ser formalmente aprovada pela gestão de topo do cliente. A Política deve ser revista em intervalos planeados de forma a garantir que a mesma se mantém adequada aos obetivos do cliente. A Política de Resposta a Incidentes deve, no mínimo abordar os seguintes pontos: - Planeamento e preparação; - Deteção e registo de eventos de segurança; - Decisão sobre eventos de segurança, nomeadamente se os mesmo constituem ou não um incidente de segurança; - Registo dos eventos de segurança; - Resposta a incidentes, incluindo investigação, resposta a situações de crise, contenção e recuperação; - Registo dos incidentes de segurança; - Constituição e responsabilidade da equipa de resposta a incidentes (equipa da organização e do cliente); - Comunicação dos incidentes. A política deve ser comunicada a todos os elementos envolvidos na prestação do serviço, designadamente a equipa da organização e a equipa interna do cliente.	Organizacionais	**A organização deve evidenciar:** **- Política documentada de resposta a incidentes, aprovada pela gestão de topo do cliente;** **- Registos de revisão e atualização periódica da política;** **- Registos da comunicação da Política.**

Referência	Requisito	Definição	Categoria	Evidências
MR.12	**Lições aprendidas**	A organização deve manter registos da revisão detalhada de incidentes após a sua resolução para identificar lições aprendidas e melhorias necessárias.	Organizacionais	**A organização deve evidenciar:** **- Relatório de análise pós-incidente, que inclua no mínimo:** **- análise das causas dos incidentes;** **- registos de reuniões de revisão pós-incidente.** **- identificação das medidas de resposta implementadas;** **- identificação de ações de melhoria.**
MR.13	**Estrutura de Resposta a Incidentes**	A organização deve estabelecer uma estrutura de resposta a incidentes, que inclua membros da organização e do cliente, no âmbito da prestação do serviço. Esta estrutura deve garantir as equipas consideradas vitais para a prestação do serviço, entre as quais: - Equipa de gestão de incidentes (IMT - Incident Management Team); - Equipa de Resposta a incidentes (IRTs - Incident response Teams); - Equipa de Gestão da Mudança; - Equipa de Gestão das vulnerabilidades; - Equipa de Gestão de crise; - Equipa de Monitorização de segurança. A organização deve documentar a estrutura de resposta a incidentes, identificando a estrutura, responsabilidades e pessoal associado à execução do serviço.	Organizacionais	**A organização deve evidenciar para cada cliente:** **- Organograma da Equipa de resposta a Incidentes;** **- Descrição de funções;** **- Matriz de atribuição de funções.**
MR.14	**Comunicação de Incidentes**	A organização deve estabelecer regras para a comunicação de incidentes ao cliente, através da criação de canais e procedimentos, bem como definir a quem deve ser comunicada a ocorrência de incidentes. A organização deve manter registos da comunicação das regras. A organização deve ainda definir as regras para a comunicação a realizar pelo cliente às partes interessadas.	Humanos	**A organização deve evidenciar:** **- Procedimento documentado de comunicação de incidentes;** **- Registos de comunicações de incidentes reportadas ao cliente;** **- Acordos de nível de serviço (SLAs) com o cliente que devem incluir procedimentos de comunicação de incidentes;** **- Registos da comunicação dos procedimentos de comunicação;** **- Procedimento documentado de comunicação de incidentes às partes interessadas.**

Referência	Requisito	Definição	Categoria	Evidências
MR.15	**Registo de Incidentes**	A organização deve garantir a criação e atualização constante de um registo detalhado de todos os incidentes de segurança, no âmbito da prestação do serviço de Resposta a Incidentes, incluindo detalhes de detecção, resposta e resolução.	Técnicos	**A organização deve evidenciar:** **- Sistema de registo de incidentes implementado e operacional;** **- Interações/Histórico detalhados dos incidentes registados;** **- Relatórios periódicos de incidentes gerados pelo sistema.**
MR.16	**Análise de Incidentes**	A organização deve documentar a metodologia a implementar desde a ocorrência do incidente até à sua recuperação. A organização deve analisar detalhadamente os incidentes de segurança, no âmbito da prestação do serviço de Resposta a Incidentes, para determinar a causa raiz e identificar as correções e/ou ações corretivas necessárias.	Técnicos	**A organização deve evidenciar:** **- Procedimentos documentados para a gestão dos incidentes;** **- Relatórios de análise de incidentes específicos;** **- Ações implementadas baseadas nas análises de incidentes.**
MR.17	**Recuperação de Incidentes**	A organização deve definir e implementar as ações necessárias para restaurar sistemas e operações, após a ocorrência de um incidente de segurança.	Técnicos	**A organização deve evidenciar:** **- Procedimentos de recuperação documentados;** **- Registos de atividades de recuperação executadas após incidentes;** **- Relatórios de recuperação com avaliações de eficácia.**
MR.18	**Período de retenção de *logs*** e evidências	A organização deve manter registos dos incidentes ocorridos, desde a sua ocorrência até à sua conclusão, inluindo *logs* . O período mínimo de retenção dos registos, deve ser até à próxima auditoria a realizar pelo organismo de certificação	Técnicos	**A organização deve evidenciar:** **- Os registos de logs de todas as ferramentas utilizadas que permitam avaliar a deteção de comportamentos anómalos desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);** **- Registos do tratamento dos incidentes.**
MR.19	**Avaliação de Impacto**	A organização deve documentar a metodologia de avaliação de impacto. A organização deve realizar a avaliação de impacto de incidentes de segurança, no âmbito da prestação do serviço.	Organizacionais	**A organização deve evidenciar:** **- Relatórios de avaliação de impacto realizados para incidentes significativos;** **- Procedimentos documentados para a realização de avaliações de impacto.**

Referência	Requisito	Definição	Categoria	Evidências
MR.20	**Planos de Resposta a Incidentes**	A organização deve elaborar e testar em intervalos planeados, os planos de resposta a incidentes de segurança, envolvendo todas as pessoas com intervenção nos planos. Os Planos de Resposta a Incidentes devem ser revistos periódicamente e formalmente aprovados pela Gestão de Topo do cliente.	Organizacionais	**A organização deve evidenciar:** **- Planos de resposta a incidentes documentados e aprovados pela gestão de topo do cliente;** **- Registo dos exercícios realizados aos planos de resposta;** **- Relatórios de exercícios e simulações de resposta a incidentes.**
MR.21	**Coordenação com Autoridades**	No âmbito da prestação do serviço, a organização deve definir procedimentos para coordenar respostas a incidentes com autoridades governamentais e regulatórias. Estes procedimentos devem ser aprovados formalmente pela Gestão de Topo do cliente e devem ser revistos em intervalos planeados.	Organizacionais	**A organização deve evidenciar:** **- Procedimentos documentados para a coordenação com autoridades;** **- Registos de comunicações e interações com autoridades durante incidentes.**
MR.22	**Avaliação de Ferramentas de Resposta**	A organização deve definir e implementar um processo de avaliação das ferramentas utilizadas para responder a incidentes de segurança. O processo de avaliaçao deve garantir o teste das ferramentas e ser realizado em intervalos planeados.	Técnicos	**A organização deve evidenciar:** **- Documentação de avaliação e seleção de ferramentas de resposta;** **- Registos de testes de ferramentas antes da implementação;** **- Relatórios de desempenho e eficácia das ferramentas em uso.**
MR.23	**Recolha de evidências Digitais**	A organização deve definir e implementar um processo de recolha de dados digitais relevantes para investigação, no âmbito da prestação de serviço ao cliente.	Técnicos	**A organização deve evidenciar:** **- *Logs* dos sistemas/aplicações afetadas;** **- Relatórios de recolha de dados;** **- Registo de acesso;** **- *Snapshot* s de memória.**
MR.24	**Análise de Malware**	A organização deve realizar uma investigação detalhada de possíveis malwares encontrados nos sistemas afetados pelo incidente.	Técnicos	**A organização deve evidenciar:** **- Relatórios de análise de *malware* ;** **- Arquivos de malware isolado;** **- Registos de quarentena;** **- Evidências de remoção.**
MR.25	**Preservação de Provas**	A organização deve definir e implementar uma política de preservação de provas. A política deve ser aprovada formalmente pela gestão de topo do cliente e revista em intervalos planeados de forma a garantir que a mesma se mantém adequada.	Organizacionais	**A organização deve evidenciar:** **- Política de preservação de provas;** **- Cópias das provas;** **- Registos da cadeia de custódia;** **- Quais os algoritmos com função *hash* utilizados na verificação de integridade;** **- *Logs* de acesso às evidências.**

Referência	Requisito	Definição	Categoria	Evidências
MR.26	**Relatórios de Investigação**	A organização deve criar pelo menos um relatório detalhado da investigações realizada, devendo conter no mínimo a narrativa detalhada das atividades realizadas e provas digitais encontradas. Os relatórios devem ser comunicados às partes interessadas relevantes na investigação do incidente.	Técnicos	**A organização deve evidenciar:** **- Relatório de investigação;** **- *Logs* de criação do relatório;** **- Registos da comunicação do relatório.**
MR.27	**Metodologia de análise forense digital**	A organização deve definir a metodologia de análise forense a utilizar. A metodologia deve estar documentada, aprovada pela gestão de topo do cliente e e revista em intervalos planeados	Técnicos	**A organização deve evidenciar:** **- A metodologia de análise forense documentada e aprovada pela gestão de topo do cliente.**
MR.28	**Verificação de Integridade de Sistemas**	A organização deve definir e implementar procedimentos para monitorizar de forma contínua a integridade dos sistemas críticos do cliente.	Técnicos	**A organização deve evidenciar:** **- *Logs* de integridade;** **- Relatórios de verificação;** **- Registo de anomalias;** **- Procedimentos de verificação.**
MR.29	**Qualificação da Equipa de Monitorização e Resposta a Incidentes**	A organização deve: - Determinar as competências necessárias das pessoas que constituem a equipa afeta à prestação do serviço de Resposta a Incidentes, assegurando que no mínimo, a equipa possua as seguintes: - Conhecimento de categorias de incidentes e respetivas respostas; - Conhecimento de danos colaterais e de estimação de impactos; - Conhecimento de exercícios de resposta e recuperação; - Conhecimento de metodologias de resposta a incidentes; - Conhecimento de planeamento de ações em situações de crise; - Conhecimento de processos e operações para gestão de incidentes, problemas e eventos; - Conhecimento de protocolos, processos e técnicas de gestão de crise; - Conhecimento de técnicas de análise de causa raiz; - Conhecimento do tempo de recuperação e de reparação estimados; - Conhecimento dos procedimentos e ferramentas de documentação e de consulta de incidentes, problemas e eventos reportados; - Conhecimento dos programas, funções e responsabilidades de resposta a incidentes; - Conhecimento dos resultados de linhas de ação e de exercícios de análise; - Conhecimento dos meios de comunicação com pessoas e entidades, internas e externas, para a gestão de incidentes. - Assegurar que essas pessoas são competentes, com base numa apropriada escolaridade, formação ou experiência; - Quando aplicável, empreender ações para que as pessoas adquiram as competências necessárias e avaliar a eficácia das ações de formação empreendidas. A organização deve manter os respetivos registos.	Humanos	**A organização deve evidenciar os registos de competências necessárias para as pessoas que constituem a equipa afeta à prestação do serviço de Resposta a incidentes, através da disponibilização de certificados e/ou demonstração da experiência profissional conforme adequado.** **A organização deve evidenciar registos de formação, se aplicável, bem como da sua eficácia.**

Referência	Requisito	Definição	Categoria	Evidências
MR.30	**Certificação da Equipa**	Pelo menos um dos elementos da equipa afeta à prestação do serviço de Resposta a Incidentes, deve possuir uma ou mais, das seguintes certificações, ou equivalente: - ISC2 CC (Certified in Cybersecurity); - CompTIA Security+ ; - ECIH (Certified in Incident Handling); - CySA+ CompTIA (Cybersecurity Analist); - CEH (Certified Ethical Hacker); - SSCP - IS2 (Systems Security Certified Practitioner); - CISSP (Certified Information Systems Security Professional); - CISM (Information Security Manager). A equivalência deve ser fundamentada pela organização.	Humanos	**A organização deve evidenciar os certificados que comprovem as certificações requeridas a pelo menos um dos elementos afetos à realização da monitorização e resposta a incidentes.** **A organização deve evidenciar os registos que suportam a fundamentação de equivalência.**

Gestão de Vulnerabilidades – GV

Referência	Requisitos	Definição	Categoria	Evidências
GV.01	**Proposta**	A organização deve manter registos de proposta para a execução dos serviços de Gestão de vulnerabilidades devendo incluir, no mínimo, a seguinte informação: - Âmbito: Identificação precisa dos sistemas, redes, aplicações e bases de dados a serem avaliados. Devem ser incluídos sistemas de terceiros, se aplicável, com devida autorização; - Objetivo: identificar o objetivo do serviço de análise de vulnerabilidades; - Requisitos da prestação de serviço: gestão de mudança, periodicidade; - Duração da prestação do serviço; - Identificação da metodologia a utilizar; - Responsabilidades: identificar a equipa de análise de vulnerabilidades e a equipa interna do cliente, se aplicável, e as responsabilidades no âmbito da proposta; - Limitações e restrições: especificar qualquer limitação, como horário da prestação do serviço, partes do sistema que não devem ser incluídos na prestação do serviço, ou outro; - Autorização formal: a proposta deve explicitar a necessidade de ser formalmente aprovada pelo cliente; - Confidencialidade: incluir disposições sobre a confidencialidade e como os dados recolhidos durante a prestação do serviço	Organizacionais	**A organização deve disponibilizar a proposta e a respetiva aceitação, se aplicável, pelo cliente para a execução da gestão de vulnerabilidades.**
GV.02	**Metodologia**	A organização deve definir e adotar a metodologia de gestão de vulnerabilidades a utilizar para a prestação do serviço, incluindo as ferramentas utilizadas. A metodologia deve conter no mínimo as seguintes fases: - Descoberta de ativos; - Prioritização de ativos; - Pesquisa de vulnerabilidades; - Análise de resultados e medidas de mitigação; - Processo contínuo de análise de vulnerabilidades. A metodologia de gestão de vulnerabilidades deve ser revista em intervalos planeados e atualizada sempre que aplicável.	Técnicos	**A organização deve evidenciar:** **- Documento descritivo da metodologia utilizada;** **- registos de análises de vulnerabilidades efetuados;** **- Listagem das ferramentas utilizadas, com identificação da versão;** **- Registos de revisão periódica da política.**
GV.03	**Relatório**	A organização deve produzir relatórios regulares sobre a gestão de vulnerabilidades e comunica-los ao cliente. No mínimo os relatórios devem conter: - Descrição detalhada da metodologia utilizada; - Número CVE (Common Vulnerabilities and Exposures), sempre que aplicável; - Pontuação CVSS (Common Vulnerability Scoring System) ou outro sistema de classificação de vulnerabilidades utilizado pela indústria; - Medidas de mitigação recomendadas.	Técnicos	**A organização deve evidenciar:** **- Relatórios regulares do processo de gestão de vulnerabilidades;** **- Processo de classificação das vulnerabilidades devidamente documentado;** **- Comunicação do relatório ao cliente.**
GV.04	**Plano de ação**	A organização deve definir e implementar um plano de ações para a mitigação de vulnerabilidades, que identifique pelo menos: - Ação a implementar; - Responsável; - Prazo para implementação; - Plano de monitorização. O plano de ação deve ser revisto em intervalos planeados e se necessário atualizado.	Organizacionais	**A organização deve evidenciar:** **- Plano de ação;** **- Registos da minitorização do plano de ação;** **- Registos da revisão do plano de ação;** **- *Logs* de implementação desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);.**

Referência	Requisitos	Definição	Categoria	Evidências
GV.05	**Política de atualizaç**	A organização deve assegurar a existência de uma política de atualizações automáticas, devendo a mesma ser aprovada formalmente pela gestão de topo do cliente. A política deve ser revista em intervalos planeados de forma a garantir que a mesma se mantém adequada aos objetivos.	Técnicos	**A organização deve evidenciar:** **- Política documentada de atualizações automáticas, aprovada pela gestão de topo do cliente;** **- Registos de revisão periódica da política;** **- *Logs* de atualizações desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);.**
GV.06	**Qualificação da equ**	A organização deve: - Determinar as competências necessárias das pessoas que constituem a equipa afeta à realização da Gestão de Vulnerabilidades, assegurando no mínimo, as seguintes: - domínio das ferramentas de diagnóstico de sistemas utilizadas na organização; - Assegurar que essas pessoas são competentes, com base numa apropriada escolaridade, formação ou experiência; - Quando aplicável, empreender ações para que as pessoas adquiram as competências necessárias e avaliar a eficácia das ações de formação empreendidas. A organização deve manter os respetivos registos.	Humanos	**A organização deve evidenciar os registos de competências necessárias para as pessoas que constituem a equipa afeta à gestão de vulnerabilidades, através da disponibilização de certificados e/ou demonstração da experiência profissional conforme adequado.** **A organização deve evidenciar registos de formação, se aplicável, bem como da sua eficácia.**
GV.07	**Certificação da equi**	Pelo menos um dos elementos da equipa afeta à realização da gestão de vulnerabilidades, deve possuir uma ou mais, das seguintes certificações, ou equivalente: - CEH (Certified Ethical Hacker); - Pentest+. A equivalência deve ser fundamentada pela organização.	Humanos	**A organização deve evidenciar os certificados que comprovem as certificações requeridas a pelo menos um dos elementos afetos à realização da gestão de vulnerabilidades.** **A organização deve evidenciar os registos que suportam a fundamentação de equivalência.**

Informações Sobre Ameaças – ISA

Referência	Requisito	Definição	Categoria	Evidência
ISA.01	**Proposta**	A organização deve manter registos de proposta para a execução dos seriços de *Threat Intelligence* , devendo incluir, no mínimo, a seguinte informação: - Âmbito: Identificação precisa do âmbito a proteger, incluíndo a(s) marca(s), pessoa(s); - Objetivo: identificar o objetivo do serviço de *Threat Intelligence* ; - Fontes de *Threat Intelligence* : identificar claramente as fontes confiáveis de inteligência de ameaças que serão utilizadas na prestação do serviço, incluindo fontes abertas, comerciais, *dark web* e parceiros; - Limitações e restrições: especificar qualquer limitação, nomeadamente o processo de validação das ações a tomar, aquando da identificação de ameaças; - Autorização formal: a proposta deve explicitar a necessidade de ser formalmente aprovada pelo cliente; - Confidencialidade: incluir disposições sobre a confidencialidade e como os dados recolhidos durante a prestação do serviço serão protegidos e utilizados.	Organizacionais	**A organização deve disponibilizar a proposta e a respetiva aceitação, se aplicável, pelo cliente para a execução do serviço de *Threat Intelligence* .**
ISA.02	**Relatórios**	A organização deve realizar relatórios regulares sobre o panorama de ameaças aplicáveis ao âmbito de atividade do cliente. Os relatórios devem ser elaborados e entregues aos clientes em intervalos planeados.	Organizacionais	**A organização deve evidenciar: - Relatórios sobre o panorama de ameaças; - A entrega dos relatórios aos clientes.**
ISA.03	**Tratamento de Informações sobre Ameaças**	A organização deve proceder ao tratamento de grandes volumes de informações sobre Ameaças, recolhidas através das fontes de *Threat Intelligence* utilizadas, em formato estruturado e não estruturado.	Técnicos	**A organização deve evidenciar: - Relatórios de processamento; - Plataformas de análise em uso.**
ISA.04	**Classificação de Ameaças**	A organização deve elaborar uma Política de Classificação de Ameaças, para classificar ameaças com base na gravidade e impacto das mesmas. A política deve ser aprovada formalmente pela gestão de topo do cliente e revista em intervalos planeados de forma a garantir que a mesma se mantém adequada.	Organizacionais	**A organização deve evidenciar: - Política de classificação de ameaças.**
ISA.05	**Monitorização contínua de ameças externas (zero days)**	A organização deve proceder à monitorização de eventos de segurança em tempo real, criando realatórios que permitam seguir e identificar tendências ao longo do tempo.	Técnicos	**A organização deve evidenciar: - *Logs* de monitorização desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a**
ISA.06	**Análise de Comportamento**	A organização deve implementar atividades de análise comportamental para detectar anomalias em rede e sistemas.	Técnicos	**A organização deve evidenciar: - Relatórios de análise comportamental; - Registos de detecção de anomalias.**
ISA.07	**Plano de Resposta a Ameaças**	A organização deve definir e implementar planos detalhados para resposta rápida e mitigação de ameaças identificadas através processo de tratamento de informações sobre ameaças. Os planos devem ser testados em intervalos planeados.	Organizacional	**A organização deve evidenciar: - Procedimentos documentados; - Exercícios simulados de resposta.**

Referência	Requisito	Definição	Categoria	Evidência
ISA.08	**Avaliação de Riscos de Ameaças**	A organização deve definir e implementar uma metodologia para realizar a avaliação dos riscos identificados através do processo de tratamento em ameaças emergentes, identificadas através do processo de tratamento de informações sobre ameaças.	Organizacional	**A organização deve evidenciar:** **- Metodologia de avaliação dos riscos;** **- Relatórios de avaliação dos riscos.**
ISA.09	**Parcerias com Comunidades de Threat Intelligence**	A organização deve participar em grupos especiais de interesse, fóruns ou entidades na área do tratamento de informações de ameaças, como ISACs.	Organizacional	**A organização deve evidenciar:** **- Registos de avaliação em grupos especiais de interesse, fóruns ou ISACs;** **- Acordos de partilha de informações (se aplicável)**
ISA.10	**Indicadores de Comprometimento (IOCs)**	A organização deve definir, documentar e implementar os IOCs para rápida detecção e resposta a ameaças, através da análise e correlação de informações sobre ameaças. Os indicadores devem ser revistos em intervalos regulares.	Técnicos	**A organização deve evidenciar:** **- A lista de IOC's definidos para o cliente;** **- *Logs* dos IOCs desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);;** **- Relatórios de incidentes correlacionados;** **- Revisão dos indicadores.**
ISA.11	**Mecanismos de Partilha de Informação**	A organização deve definir a estrutura de dados,a utilizar na partilha de informações sobre ameaças com outras entidade.	Organizacional	**A organização deve evidenciar:** **- Estrutura de dados definida;** **- Acordos de partilha de informações,** **- *Logs* de partilha de informação desde a última auditoria de certificação, após a concessão da certificação (aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses);.**
ISA.12	**Mecanismo de Atribuição de Ameaças**	A organização deve definir e implementar uma política de Classificação e atribuição de ameças a grupos ou indíduos.	Técnicos	**A organização deve evidenciar:** **- Política de classificação e atribuição de ameaças;** **- Relatórios de classificação e atribuição de ameaças.**

Referência	Requisito	Definição	Categoria	Evidência
ISA.13	**Qualificação da Equipa de Informações sobre ameaças**	A organização deve: -Ddeterminar as competências necessárias das pessoas que constituem a equipa afeta à prestação do serviço de Informações sobre ameaças, assegurando que no mínimo, a equipa possua as seguintes: - Conhecimento da estrutura, abordagem e estratégia das ferramentas de exploração de vulnerabilidades (e.g., *sniffers* , *keyloggers*) e as técnicas subjacentes (e.g., obtenção de acesso *backdoor* , recolha/exfiltração de dados, análise de vulnerabilidades de sistemas); - Conhecimento da linguagem especializada do alvo (e.g., acrónimos, jargões, terminologia técnica, palavras de código); - Conhecimento das ameaças e dos sistemas alvo; - Conhecimento das diferentes classes de ataques (e.g., passivo, ativo, ataque interno, ataque distribuído); - Conhecimento das disciplinas de informações de ameaças; - Conhecimento das fases de um ciberataque (e.g., reconhecimento, *scanning* , enumeração, ganho de acesso, escalamento de acesso, mantimento de acesso, exploração de rede, encobrimento de evidências); - Conhecimento das ferramentas e técnicas de comunicação dos alvos; - Conhecimento das táticas internas de antecipação e de simulação de ameaças; - Conhecimento de alvos dinâmicos (não estudados, não planeados) e alvos deliberados (estudados, planeados); - Conhecimento de alvos, incluindo eventos relacionados, perfis de comunicação, agentes de ameaça, história (língua, cultura) e/ou contexto; - Conhecimento de análise de código binário; - Conhecimento de análise e caracterização de malwares; - Conhecimento de comportamentos físicos e fisiológicos que podem indicar atividade suspeita ou anormal; - Conhecimento de conceitos e metodologias de análise de malware; - Conhecimento de conceitos e técnicas de engenharia reversa em *hardware* e *software* ; - Conhecimento de contramedidas para riscos de segurança identificados; - Conhecimento de estratégias e ferramentas de pesquisa de alvos; - Conhecimento de ferramentas de análise de *malware;*	Humanos	**A organização deve evidenciar os registos de competências necessárias para as pessoas que constituem a equipa afeta à prestação do serviço de informações sobre ameaças, através da disponibilização de certificados e/ou demonstração da experiência profissional conforme adequado.** **A organização deve evidenciar registos de formação, se aplicável, bem como da sua eficácia.**
	Cont.	- Conhecimento de mecanismos de atribuição de tarefas; - Conhecimento de mecanismos que permitem a recolha de informação; - Conhecimento de níveis de confiança das informações de ameaça; - Conhecimento de perfis de comunicação dos alvos, e seus elementos (e.g., associações, atividades, infraestrutura de comunicação); - Conhecimento de princípios e práticas relacionados com o desenvolvimento de alvos (e.g., estudo pormenorizado dos seus componentes, localizações, associações, sistemas de comunicação, infraestruturas); - Conhecimento de processos autorizados de disseminação de informações de ameaças; - Conhecimento de processos de atribuição de tarefas para recolha de ativos; - Conhecimento de processos e técnicas de tradução; - Conhecimento de referências culturais, dialetos, expressões, idiomas e abreviaturas; - Conhecimento de requisitos de recursos humanos relacionados com informações de ameaça (e.g., logística, comunicações, restrições legais); - Conhecimento de sistemas de atribuição de tarefas em relação às informações de ameaça; - Conhecimento de técnicas de comunicação dissimuladas; - Conhecimento de técnicas e estratégias de evasão; - Conhecimento de vetores de ataques atuais e emergentes; - Conhecimento do ambiente de ameaças da organização; - Conhecimento do ciclo de feedback nos processos de recolha de dados; - Conhecimento do ciclo de targeting;		

Referência	Requisito	Definição	Categoria	Evidência
	Cont.	- Conhecimento do formato de dados estabelecido no plano de recolha de informações de ameaça da organização; - Conhecimento do processo de desenvolvimento de alvo (i.e., conceitos, funções, responsabilidades, produtos); - Conhecimento do processo de desenvolvimento de lista de alvo (i.e., candidatos, restritos); - Conhecimento do processo de produção de informações de ameaça; - Conhecimento do suporte que as informações de ameaças fornecem ao planeamento, execução e avaliação; - Conhecimento dos alvos de ataque, agentes de ameaça cibernéticos e procedimentos utilizados nos ataques; - Conhecimento dos fatores chave do ambiente operacional e das ameaças; - Conhecimento dos fatores de risco que podem impactar as operações de recolha de dados; - Conhecimento dos métodos e procedimentos do alvo; - Conhecimento dos métodos e técnicas de ataque; - Conhecimento dos níveis de confiança das informações de ameaça; - Conhecimento dos objetivos dos modelos de alvo; - Conhecimento dos princípios, políticas e procedimentos de recolha de informações de ameaça, incluindo restrições legais e autoridades legais; - Conhecimento dos procedimentos de verificação e validação do alvo; - Conhecimento dos processos de preparação de informações de ameaça do meio ambiente e processos similares; - Conhecimento dos processos de recolha de informações de ameaça de alvo; - Conhecimento dos produtos necessários para o planeamento operacional de cibersegurança; - Conhecimento dos recursos e limitações das informações de ameaça; - Conhecimento dos tipos de ciberatacantes (e.g., script kiddies, ameaças internas, ameaças patrocinadas por Estados); - Assegurar que essas pessoas são competentes, com base numa apropriada escolaridade, formação ou experiência;		
ISA.14	**Certificação da Equipa**	Pelo menos um dos elementos da equipa afeta à prestação do serviço de Informações sobre ameaças, deve possuir uma ou mais, das seguintes certificações, ou equivalente: - OSTH (Offsec Threat Hunter); - eCTHP Certification (Certified Threat Hunting Professional). A equivalência deve ser fundamentada pela organização.	Humanos	**A organização deve evidenciar os certificados que comprovem as certificações requeridas a pelo menos um dos elementos afetos à realização do serviço de informações sobre ameaças. A organização deve evidenciar os registos que suportam a fundamentação de**

Teste Intrusão - TI

Referência	Requisitos	Definição	Categoria	Evidências	Notas
TI.01	**Proposta**	A organização deve manter registos de proposta para a execução do teste de intrusão, a qual deve incluir, no mínimo, a seguinte informação: - Âmbito: especificar claramente qual(ais) sistema(s), rede(s), aplicação(ões) a ser(em) testado(s); (infraestrutura, wi-fi, IoT, aplicações web e/ou mobile); - Objetivo: identificar o objetivo do teste; - Identificação da metodologia a utilizar; **(Nota 1)** - Tipologia do teste: especificar a tipologia de teste a realizar: white box, grey box, black box; - Prazo de execução: identificar o periodo de tempo necessário para a realização do teste de intrusão e apresentação dos respetivos resultados; - Responsabilidades: identificar a equipa de testes e a equipa interna do cliente e as responsabilidades no âmbito da proposta; - Limitações e restrições: especificar qualquer limitação, como horário permitido para testes, partes do sistema que não devem ser testadas, ou outro; - Autorização formal: a proposta deve explicitar a necessidade de ser formalmente aprovada pelo cliente; - Confidencialidade: incluir disposições sobre a confidencialidade e como os dados recolhidos durante os testes serão protegidos e utilizados; - Entregáveis: especificar claramente os entregáveis resultantes do teste de intrusão, que deverão incluir no mínimo um relatório e documentação técnica.	Organizacionais	A organização deve disponibilizar a proposta e a respetiva aceitação, se aplicável, pelo cliente para a execução do teste de intrusão.	**(Nota 1): Como metodologias de referência, a organização deve considerar:** **- OWASP Web Security Testing Guide / Mobile Security Testing Guide** **- PCI/DSS penetration testing guidance** **- https://docs-prv.pcisecuritystandards.org/Guidance%20Document/Penetration%20Testing/Penetration-Testing-Guidance-v1_1.pdf** **- NIST SP800-115 - https://csrc.nist.gov/pubs/sp/800/115/final** **- ISACA P8**
TI.02	**Relatório**	A organização deve entregar um relatório para cada teste de intrusão que permita apresentar o trabalho realizado. O relatório deve conter, no mínimo os seguintes elementos: - Âmbito do teste de intrusão; - Objetivo do teste de intrusão; - Datas de execução do teste de intrusão; - Descrição detalhada da metodologia utilizada; - Equipa responsável pela realização do teste de intrusão; - Pessoa responsável pela aprovação do relatório; - Descrição das vulnerabilidades identificadas, que deve incluir no mínimo: a) Designação; b) Número CVE (*Common Vulnerabilities and Exposures*), sempre que aplicável; c) Pontuação CVSS (Common Vulnerability Scoring System), ou outro sistema de classificação de vulnerabilidades utilizado pela indústria; d) Impacto; e) Recomendações: ações a implementar para mitigar a(s) vulnerabilidade(s) encontrada(s); f) Outras recomendações: outras ações que sejam importantes para a segurança do(s) sistema(s), rede(s), aplicação(ões) em teste.	Técnicos	A organização deve disponibilizar o relatório do teste de intrusão entregue ao cliente.	

Referência	Requisitos	Definição	Categoria	Evidências	Notas
TI.03	**Documentação técnica**	A organização deve entregar a documentação técnica que considere apropriada para evidenciar a forma como o teste de intrusão foi realizado. A documentação técnica a entregar deve conter, no mínimo, os seguintes elementos: - identificação das ferramentas usadas para a realização do teste intrusão e respetiva versão, - metodologia: descrição detalhada da metodologia utilizada; - narrativa técnica: descrição detalhada das várias atividades realizadas, com a inclusão de evidências. - descrição das vulnerabilidades identificadas, que deve incluir no mínimo: a) designação, b) número CVE (Common Vulnerabilities and Exposures), sempre que aplicável, c) pontuação CVSS (Common Vulnerability Scoring System), ou outro sistema de classificação de vulnerabilidades utilizado pela indústria, d) Impacto, e) recomendações: ações a implementar para mitigar a(s) vulnerabilidade(s) encontrada(s). f) outras recomendações: outras ações que sejam importantes para a segurança do(s) sistema(s), rede(s), aplicação(ões) em teste.	Técnicos	A organização deve manter registos da documentação técnica entregue ao cliente, para cada teste de intrusão realizado.	
TI.04	**Período de retenção de *logs***	Registos dos *logs* de todas as ferramentas utilizadas, cujo período mínimo de retenção deve ser até à próxima auditoria a realizar pelo organismo de certificação.	Técnicos	A organização deve evidenciar os registos de *logs* de todas as ferramentas utilizadas no teste de intrusão, desde a realização do teste até à próxima auditoria a realizar pelo organismo de certificação. Aquando da auditoria de concessão, a Organização deve evidenciar registos desde, pelo menos, os útimos 6 meses;	
TI.05	**Qualificação da equipa**	A organização deve: - Determinar as competências necessárias das pessoas que constituem a equipa afeta à realização do teste de intrusão, assegurando no mínimo, as seguintes: - domínio das ferramentas de diagnóstico de sistemas utilizadas na organização; - domínio das técnicas de identificação de vulnerabilidades utilizadas na organização; - domínio dos métodos de teste e avaliação de sistemas, redes, aplicações utilizados na organização. - Assegurar que essas pessoas são competentes, com base numa apropriada escolaridade, formação ou experiência; - Quando aplicável, empreender ações para que as pessoas adquiram as competências necessárias e avaliar a eficácia das ações de formação empreendidas. A organização deve manter os respetivos registos.	Humanos	A organização deve evidenciar os registos de competências necessárias para as pessoas que constituem a equipa afeta à realização do teste de intrusão, através da disponibilização de certificados e/ou demonstração da experiência profissional conforme adequado. A organização deve evidenciar registos de formação, se aplicável, bem como da sua eficácia.	

Referência	Requisitos	Definição	Categoria	Evidências	Notas
TI.06	**Certificação da equipa**	Pelo menos um dos elementos da equipa afeta à realização do teste de intrusão, deve possuir uma ou mais, das seguintes certificações, ou equivalente: - CEH (Certified Ethical Hacker); - OSCP (Offensive Security Certified Professional); - CISSP (Certified Information Systems Security Professional). A equivalência deve ser fundamentada pela organização.	Humanos	A organização deve evidenciar os certificados que comprovem as certificações requeridas a pelo menos um dos elementos afetos à realização do teste de intrusão. A organização deve evidenciar os registos que suportam a fundamentação de equivalência.	