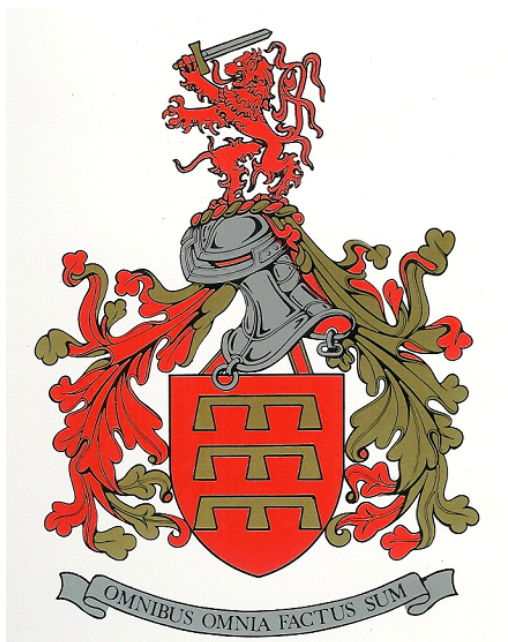


MINISTÉRIO DA DEFESA NACIONAL
EXÉRCITO PORTUGUÊS
INSPEÇÃO-GERAL DO EXÉRCITO



Listas de Verificação

Inspeção de Segurança Militar, Comunicações e Sistemas de Informação

A - GESTÃO DA SEGURANÇAP: **A1 - ORGANIZAÇÃO**P: **A1.1 - Estrutura de Segurança**P:

- | | | |
|---|--------------------------|-----------------------------------|
| 1 - Verificar se a estrutura de segurança está organizada de acordo com os normativos em vigor. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 2 - Verificar se os elementos da estrutura SegMil estão nomeados em Ordem de Serviço (OS). | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 3 - Verificar se o Custódio Cripto e Custódio Cripto Substituto estão nomeados OS. | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 4 - Verificar se a U/E/O tem Administrador de Rede Local nomeado em OS. | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 5 - Verificar se existem normativos (e.g NEP) para os elementos da estrutura SegMil, que regulem as respetivas atribuições e responsabilidades. | Av: <input type="text"/> | P: <input type="text" value="3"/> |

A1.2 - Procedimentos de SrgurançaP:

- | | | |
|---|--------------------------|-----------------------------------|
| 1 - Verificar se o relatório da Inspeção anterior esta distribuído pela estrutura SegMil e disponível para consulta. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 2 - Verificar a existência de diretivas/NEP/Instruções de SEGMIL, adaptadas às condições específicas da U/E/O, são do conhecimento de todos os elementos que delas tenham necessidade de conhecer e estão reunidas numa única publicação. | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 3 - Verificar se as Diretivas/NEP/Instruções são revistas e atualizadas regularmente. | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 4 - Verificar se as violações e/ou quebras de segurança são devidamente reportadas (RELIM) e efetuada a Investigação de Segurança. | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 5 - Verificar se existem diretivas/NEP/Instruções relativas aos procedimentos na entrada de Forças e Elementos Armados na U/E/O. | Av: <input type="text"/> | P: <input type="text" value="1"/> |
| 6 - Verificar se existem diretivas/NEP/Instruções relativas aos procedimentos a adotar em caso de suspeita de crime no interior da U/E/O e com os Órgãos de Polícia Criminal. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 7 - Verificar se existem diretivas/NEP/Instruções relativas aos procedimentos para manuseamento de correio suspeito. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 8 - Verificar se existem diretivas/NEP/Instruções relativas às medidas e procedimentos de segurança a adotar pela U/E/O em caso de tentativa de intrusão ou de intrusão efetiva. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 9 - Verificar se existem diretivas/NEP/Instruções relativas à organização e produção do sistema de Identificação de Pessoal e Forças Militares na U/E/O. | Av: <input type="text"/> | P: <input type="text" value="3"/> |

A1.3 - Plano de SegurançaP:

- | | | |
|---|--------------------------|-----------------------------------|
| 1 - Verificar se o plano de segurança e/ou contingência respeita os princípios essenciais necessários à sua operacionalização. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 2 - Verificar se o plano de segurança inclui em anexo, pelo menos, o plano de defesa e que considere os requisitos em referência. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 3 - Verificar se o plano de segurança é do conhecimento geral. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 4 - Verificar se o Comando e Controlo é garantido em todas as fases de implementação do Plano. | Av: <input type="text"/> | P: <input type="text" value="3"/> |
| 5 - Verificar se todos os militares têm conhecimento da sua responsabilidade na execução do Plano de Defesa. | Av: <input type="text"/> | P: <input type="text" value="2"/> |
| 6 - Verificar se os planos são treinados. | Av: <input type="text"/> | P: <input type="text" value="3"/> |

B - SEGURANÇA FÍSICAP: **B1 - MEDIDAS DE SEGURANÇA FISICA**P: **B1.1 - Genéricas**P:

1 - Verificar se as chaves e combinações de segredo dos acessos às Áreas de Segurança de Classe 1 e 2 são consideradas chaves de segurança e são geridas como tal.

Av: P:

2 - Verificar se é mantido um registo de entradas a pessoal não pertencente à U/E/O (incluindo pessoal auxiliar, de limpeza etc).

Av: P:

3 - Verificar se são usados de cartões de acesso na U/E/O e da forma adequada.

Av: P:

4 - Verificar se são realizadas rondas e verificações por parte dos Elementos de Segurança no interior de áreas de segurança ou nas imediações das mesmas, cumprindo os requisitos em referência.

Av: P:

5 - Verificar se a U/E/O é capaz de destacar uma força de reação com um mínimo de dois elementos. A força deve responder a alarmes sonoros ou sinais de emergência, devendo ser devidamente treinada e testada.

Av: P:

6 - Verificar se são cumpridos os requisitos mínimos para armazenamento de Informação Classificada (IC).

Av: P:

7 - Verificar se existe um registo escrito de cada combinação de segredo conservado em envelopes (Mod G-12) lacrados e confiados à guarda da entidade de segurança apropriada.

Av: P:

8 - Verificar se o claviculário da U/E/O tem uma cópia lacrada de cada chave das áreas de segurança e restritas.

Av: P:

9 - Verificar se as chaves e os registos das combinações de segredo das casas-fortes e dos contentores de segurança beneficiam de uma proteção tão rigorosa quanto a das matérias a que dão acesso.

Av: P:

10 - As combinações de segredo são mudadas, no mínimo, todos os 6 meses e/ou sempre que haja mudança de pessoal com conhecimento dos mesmos e/ou quando se tenha verificado qualquer quebra de segurança ou se suspeite dessa possibilidade.

Av: P:

11 - Verificar se são cumpridos os requisitos de segurança na abertura de Contentores de Segurança e seu registo

Av: P:

12 - Verificar se existem procedimentos no que respeita à segurança nos gabinetes em normativo próprio (exemplo NEP).

Av: P:

13 - Verificar se existem salas de reuniões e de conferência e se reúnem as medidas de segurança necessárias.

Av: P:

14 - Verificar a existência de alimentação elétrica de reserva, com arranque e troca automática, em caso de falha de energia (e.g. gerador).

Av: P: **B2 - DEFESA AFASADA**P: **B2.1 - Perímetro Defensivo**P:

1 - Verificar se existe vedação com as características das ISM ao longo de todo o perímetro.

Av: P:

2 - Verificar se existem sistemas de videovigilância (VV) cobrindo todo o perímetro e cumprem os requisitos necessários.

Av: P:

3 - Verificar se existe iluminação de perímetro apropriada.

Av: P:

4 - Verificar se existem painéis identificativos de área militar e aplicados de forma adequada.

Av: P: **B2.2 - Postos Principais de Acesso à U/E/O (e.g. Posta de Armas)**P:

1 - Verificar se o(s) portão(ões) de acesso mantêm as mesmas condições de segurança do restante perímetro.

Av: P:

2 - Verificar se a estrutura da instalação cumpre os requisitos de construção através de materiais que lhes configurem maior resistência.

Av: P:

3 - Verificar a existência de videovigilância a cobrir os acessos pedonal, de viatura e a área envolvente.

Av: P:

4 - Verificar se existe uma área exterior de espera e retorno para veículos para realizar revistas e buscas, quando necessário.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
5 - Verificar se existe sistema de controlo de acessos apropriado nas entradas pedonal e de viaturas da E/U/O.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
6 - Verificar se está afixada sinalética em vigor chamando a atenção do pessoal e visitantes para os aspetos de segurança (identificação, revista a pessoas, estado de alerta e VV).	Av:	<input type="text"/>	P:	<input type="text" value="1"/>
7 - Verificar se existe iluminação interior e exterior apropriada.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
8 - Verificar se está contemplado um parque de viaturas para as visitas.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
9 - Verificar se o posto de controlo de acessos é guarnecido por militares, e funcionam de forma ininterrupta.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
10 - Verificar se existem ligações GSM, TPF ou alternativas (alarme de pânico) com o Graduado de Serviço (Oficial de Dia/Cmdt da Guarda/Sargento de dia/outro)	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
11 - Verificar se existe um local condigno, destinado à receção de visitas pessoais para os militares que servem na U/E/O e contemplado em NEP.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
12 - Verificar se as condições de armazenamento e transporte do armamento e munições utilizados pelo pessoal em serviço de segurança cumprem o preconizado superiormente.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
13 - Verificar se as condições de municiamento das armas do pessoal em serviço de segurança cumprem o preconizado superiormente.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
14 - Verificar se estão afixados junto à Porta de Armas os cartazes sobre operações de segurança ao armamento ligeiro do exército.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>

B3 - ÁREAS DE SEGURANÇA - CLASSE 2

P:

B3.1 - Gabinete de Serviço

P:

1 - Verificar se a construção da estrutura é sólida, nomeadamente: betão, tijolo ou material equivalente.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
2 - Verificar se as janelas e outras aberturas cumprem com os requisitos necessários.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
3 - Verificar se a porta de acesso exterior é no mínimo de classe de resistência 3 de acordo com a norma EN 1627 e cumpre com os restantes requisitos necessários.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
4 - Verificar se a(s) fechadura(s) cumpre(m) com os requisitos necessários, nomeadamente o sistema de abertura elétrico, utilizado no controlo de acessos, se é no mínimo de resistência de 300 Kg-f.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
5 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência (se aplicável) e emite os alertas na sala de monitorização do SICAVE.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
6 - Verificar se existem câmaras a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
7 - Verificar se existe um sistema de salvo-conduto (cartão de acesso) e garante os requisitos necessários.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
8 - Verificar se esta área possui iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
9 - Verificar se está afixada a placa identificadora da Área de Segurança de Classe 2, na porta ou na parede a 10 cm da aduela esquerda.	Av:	<input type="text"/>	P:	<input type="text" value="1"/>

B3.2 - SOIS

P:

1 - Verificar se a construção da estrutura é sólida, nomeadamente: betão, tijolo ou material equivalente.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
2 - Verificar se as janelas e outras aberturas cumprem com os requisitos necessários.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
3 - Verificar se a porta de acesso exterior é no mínimo de classe de resistência 3 de acordo com a norma EN 1627 e cumpre com os restantes requisitos necessários.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
4 - Verificar se a(s) fechadura(s) cumpre(m) com os requisitos necessários, nomeadamente o sistema de abertura elétrico, utilizado no controlo de acessos, se é no mínimo de resistência de 300 Kg-f.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>

5 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência (se aplicável) e emite os alertas na sala de monitorização do SICAVE.

Av: P: 3

6 - Verificar se existe sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.

Av: P: 3

7 - Verificar se existe um sistema de salvo-conduto (cartão de acesso) e garante os requisitos necessários.

Av: P: 3

8 - Verificar se esta área possui iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.

Av: P: 2

9 - Verificar se está afixada a placa identificadora da Área de Segurança de Classe 2, na porta ou na parede a 10 cm da aduela esquerda.

Av: P: 1

B3.3 - Outras Áreas Classe II

P: 1

1 - Verificar se a construção da estrutura é sólida, nomeadamente: betão, tijolo ou material equivalente.

Av: P: 3

2 - Verificar se as janelas e outras aberturas cumprem com os requisitos necessários.

Av: P: 3

3 - Verificar se a porta de acesso exterior é no mínimo de classe de resistência 3 de acordo com a norma EN 1627 e cumpre com os restantes requisitos necessários.

Av: P: 3

4 - Verificar se a(s) fechadura(s) cumpre(m) com os requisitos necessários, nomeadamente o sistema de abertura elétrico, utilizado no controlo de acessos, se é no mínimo de resistência de 300 Kg-f.

Av: P: 3

5 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência (se aplicável) e emite os alertas na sala de monitorização do SICAVE.

Av: P: 3

6 - Verificar se existe sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.

Av: P: 3

7 - Verificar se existe um sistema de salvo-conduto (cartão de acesso) e garante os requisitos necessários.

Av: P: 3

8 - Verificar se esta área possui iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.

Av: P: 2

9 - Verificar se está afixada a placa identificadora da Área de Segurança de Classe 2, na porta ou na parede a 10 cm da aduela esquerda.

Av: P: 1

B4 - ÁREAS DE SEGURANÇA - CLASSE 1

P: 1

B4.1 - Posto de Controlo de Informação Classificada (PCC)

P: 1

1 - Verificar se a construção da estrutura é sólida, nomeadamente: betão, tijolo ou material equivalente.

Av: P: 3

2 - Verificar se a porta de acesso exterior cumpre com os requisitos apropriados.

Av: P: 3

3 - Se existir porta exclusivamente como saída de emergência. Caso exista, não permite a sua abertura a partir do exterior.

Av: P: 3

4 - Verificar se o sistema de abertura elétrico, utilizado no controlo de acessos, é no mínimo de resistência de 500 Kg-f.

Av: P: 3

5 - Verificar se todas as janelas e outras aberturas situadas a menos de 5,5 metros de altura do solo, nomeadamente tetos/telhados, lajes, parapeitos ou tubos de drenagem de águas pluviais estão protegidas conforme as ISM.

Av: P: 3

6 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência, se aplicável e emite os alertas na sala do SICAVE.

Av: P: 3

7 - Verificar se existe sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.

Av: P: 3

8 - Verificar se existe um sistema de controlo de entradas por dupla autenticação, nomeadamente, cartão eletrónico e PIN ou sistema de leitura biométrica.

Av: P: 3

9 - Verificar se está afixada no seu interior, uma lista de acessos permanentes autorizados àquela área, devendo os movimentos de todas as pessoas que não constarem da referida lista, ser registados e assinados.

Av: P: 2

10 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma. Av: P: 2

11 - Verificar se existe identificação de Área de Segurança de Classe 1 e painéis informativos de entrada em Áreas de Segurança, na porta ou na parede. Av: P: 1

B4.2 - Sala Tecnica do SICAVE

P: 1

1 - Verificar se a construção da estrutura é sólida, nomeadamente: betão, tijolo ou material equivalente. Av: P: 3

2 - Verificar se a porta de acesso exterior cumpre com os requisitos apropriados. Av: P: 3

3 - Se existir porta exclusivamente como saída de emergência. Caso exista, não permite a sua abertura a partir do exterior. Av: P: 3

4 - Verificar se o sistema de abertura elétrico, utilizado no controlo de acessos, é no mínimo de resistência de 500 Kg-f. Av: P: 3

5 - Verificar se todas as janelas e outras aberturas situadas a menos de 5,5 metros de altura do solo, nomeadamente tetos/telhados, lajes, parapeitos ou tubos de drenagem de águas pluviais estão protegidas conforme as ISM. Av: P: 3

6 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência, se aplicável e emite os alertas na sala do SICAVE. Av: P: 3

7 - Verificar se existe sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna. Av: P: 3

8 - Verificar se existe um sistema de controlo de entradas por dupla autenticação, nomeadamente, cartão eletrónico e PIN ou sistema de leitura biométrica. Av: P: 3

9 - Verificar se está afixada no seu interior, uma lista de acessos permanentes autorizados àquela área, devendo os movimentos de todas as pessoas que não constarem da referida lista, ser registados e assinados. Av: P: 3

10 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma. Av: P: 2

11 - Verificar se existe identificação de Área de Segurança de Classe 1 e painéis informativos de entrada em Áreas de Segurança, na porta ou na parede. Av: P: 1

B5 - ÁREAS RESTRITAS

P: 1

B5.1 - AMG

P: 1

1 - Verificar se a AMG dispõe de dois (02) compartimentos, um de acesso controlado e outro de acesso proibido, devidamente separados e todas estas áreas sinalizadas conforme com as placas informativas (Área restrita, controlada e proibida). Av: P: 3

2 - Verificar se no interior da área proibida está afixada uma lista de acessos permanentes autorizados àquela área, devendo os movimentos de todas as pessoas que não constarem da referida lista, ser registados e assinados. Av: P: 2

3 - Caso existam portas utilizadas exclusivamente como saídas de emergência, verificar que estas não permitem a sua abertura a partir do exterior, ficando assegurada apenas a sua abertura a partir do interior. Av: P: 3

4 - Verificar se a área cumpre com os requisitos das características físicas necessárias. Av: P: 3

5 - Verificar se as janelas estão protegidas com grade de ferro dispostas num quadrado soldado, ligado firmemente à estrutura da janela ou parede. As barras deverão ter no mínimo 20 mm de diâmetro e distarem entre si cerca de 15 cm. Av: P: 3

6 - Verificar se o acesso à AMG (por parte dos quarteleiros e responsáveis pela AMG) é sempre, no mínimo, com dupla autenticação (por exemplo o recurso a cartão e a código). Av: P: 3

7 - Verificar se o quarteleiro designado para o serviço diário mantém na sua posse uma chave da área proibida e outra da área controlada, garantindo os requisitos apropriados. Av: P: 3

8 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência, se aplicável e emite os alertas na sala do SICAVE. Av: P: 2

9 - Verificar se existem dispositivos de segurança nos armeiros que permitam trancar as armas no lugar. Av: P: 3

10 - Verificar se a instalação possui como meio supletivo um sistema de videoporteiro, na porta de acesso ao exterior, com abertura, que permita a segurança do quarteleiro e a salvaguarda da área proibida no momento da abertura da porta da área controlada/porta exterior.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
11 - Verificar se existe um sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
12 - Verificar se a instalação possui os meios supletivos de segurança no âmbito do Safety necessários à salvaguarda do material e equipamento.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
13 - Verificar se as portas apresentam uma estrutura sólida e no mínimo de classe de resistência 3, 4 e 5 de acordo com a norma EN 1627 ou equivalente e conforme o modelo da AMG (ALFA ou BRAVO).	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
14 - Verificar se os sistemas de abertura elétrica, utilizados no controlo de acessos, são no mínimo de resistência de 300 Kg-f e/ou 500 Kg-f (dependendo o modelo da AMG (ALFA ou BRAVO).	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
15 - Verificar se existe um sistema de controlo de acessos eletrónicos, no mínimo com dupla autenticação, integrado com a sala de monitorização SICAVE.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
16 - Verificar se o levantamento de materiais das AMG é efetuado através de recibos/requisições (em duplicado), onde conste a identificação do militar requisitante.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
17 - Verificar se existem NEP explícitas e pormenorizadas que regulem o correto armazenamento de Armamento e Equipamento Militar, bem como o bom funcionamento da AMG.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
18 - Verificar se existem munições e armamento para a defesa imediata da AMG e estão controlados e armazenados consoante o preconizado superiormente.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
19 - Verificar se existe o registo atualizado das conferências semanais detalhadas de, no mínimo, um tipo de material em arrecadação, para deteção de possíveis falhas.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
20 - Verificar se estão afixados junto à AMG os cartazes sobre operações de segurança ao armamento ligeiro do Exército.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
21 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
B5.2 - PAIOL / PAIOLIM			P:	<input type="text" value="1"/>
1 - Verificar se a vedação do perímetro no mínimo de 2,15 metros de altura e contempla um elemento em "Y" ou equivalente, com, pelo menos, 40 cm de comprimento que suporte rolos de arame farpado ou laminado ("concertina") galvanizado.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
2 - Verificar se a iluminação periférica ilumina o perímetro com uma luz uniforme e contínua.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
3 - Verificar se o Portão de Acesso ao Perímetro do Paiol é, no mínimo, tão robusto quanto a estrutura que delimita o perímetro.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
4 - Verificar se cada Paiol possui um sistema de controlo de acessos à entrada da área controlada e da área proibida, sendo que nesta última deverá ser de dupla autenticação.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
5 - Verificar se existe videovigilância focada nas portas nas entradas das áreas Restrita, Controlada e Proibida, possibilitando, também, vigilância em período noturno.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
6 - Verificar se existe afixada no seu interior, uma lista de acessos permanentes autorizados àquela área, devendo os movimentos de todas as pessoas que não constarem da referida lista, ser registados e assinados.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
7 - Verificar se existe sinalética vigente a identificar a área restrita.	Av:	<input type="text"/>	P:	<input type="text" value="1"/>
8 - Verificar se existe alarme anti-intrusão dentro do Paiol, se está de acordo com as diretivas ATEX e emite os alertas na sala de monitorização do SICAVE.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
9 - Verificar se as janelas estão protegidas com grade de ferro dispostas num quadrado soldado, ligado firmemente à estrutura da janela ou parede. As barras deverão ter no mínimo 20 mm de diâmetro e distarem entre si cerca de 15 cm. O vidro das janelas não deverá permitir observação para o interior.	Av:	<input type="text"/>	P:	<input type="text" value="3"/>
10 - Verificar se existem NEP explícitas e pormenorizadas que regulem o correto armazenamento de Munições e Explosivos e bom funcionamento do Paiol.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>
11 - Verificar se a instalação possui os meios supletivos de segurança no âmbito do Safety necessários à salvaguarda do material e equipamento.	Av:	<input type="text"/>	P:	<input type="text" value="2"/>

12 - Verificar se existe o registo atualizado das conferências de todo o material armazenado dentro do Paiol, bem como a verificação de todo o material de Security & Safety, no mínimo de três em três meses.

Av: P: 2

B5.3 - Sala de Monitorização do SICAVE

P: 1

1 - Verificar se existe sinalética vigente a identificar como Área Restrita.

Av: P: 1

2 - Verificar se existe um sistema de controlo de acessos (eletrónico ou manual).

Av: P: 3

3 - Verificar se existe um sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.

Av: P: 2

4 - Verificar se a operação de monitorização é ininterrupta 24/24H e esta guardada permanentemente, com pelo menos um elemento de segurança.

Av: P: 3

5 - Verificar se os equipamentos disponíveis para vigiar, detetar, visualizar e gravar imagens, alertam esta sala quando uma instalação ou área de segurança for objeto de intrusão.

Av: P: 3

6 - Verificar se existe ligação a uma fonte de alimentação em área protegida que garanta, sem interrupções o seu funcionamento em qualquer situação de emergência.

Av: P: 3

7 - Verificar se as imagens do CCTV não são observadas do exterior.

Av: P: 2

8 - Verificar se existem meios de comunicação para manter uma ligação permanente com o Posto de Controlo de Acessos/Portas de Armas/Portaria, caso se aplique.

Av: P: 2

9 - Verificar se existe uma planta da U/E/O para efeitos de referência e reação para casos de intrusão ou anomalia técnica.

Av: P: 2

B5.4 - Gerador

P: 1

1 - Verificar se existe sinalética vigente a identificar como Área Restrita.

Av: P: 1

2 - Verificar se existe um sistema de controlo de acessos (eletrónico ou manual).

Av: P: 3

3 - Verificar se existe alarme de intrusão cobrindo os acessos à área e emite os alertas na sala do SICAVE.

Av: P: 3

4 - Verificar se existe um sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.

Av: P: 3

5 - Verificar se existe uma barreira perimétrica que evite qualquer intrusão.

Av: P: 3

6 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.

Av: P: 2

B5.5 - Outras Áreas Restritas

P: 1

1 - Verificar se existe sinalética vigente a identificar como Área Restrita.

Av: P: 1

2 - verificar se existe um sistema de controlo de acessos (eletrónico ou manual).

Av: P: 3

3 - Verificar se existe alarme de intrusão cobrindo os acessos à área e emite os alertas na sala do SICAVE.

Av: P: 3

4 - Verificar se existe um sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.

Av: P: 3

5 - Verificar se existe uma barreira perimétrica que evite qualquer intrusão.

Av: P: 3

6 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.

Av: P: 2

C - SEGURANÇA DA INFORMAÇÃOP: 1**C1 - TRATAMENTO DE INFORMAÇÃO CLASSIFICADA**P: 1**C1.1 - Classificação e Preparação de Documentos**P: 1

1 - Verificar se o acesso à informação classificada é estabelecido na base da "necessidade de conhecer" e se existem NEP/IP, diretrizes objetivas relativas à existência de IC.

Av: P: 3

2 - Verificar se os documentos classificados apresentam graus de classificação de segurança adequados conforme normativo em referência.

Av: P: 2

3 - Verificar se os documentos classificados com os diferentes graus foram atribuídos pelas corretas entidades.

Av: P: 3

4 - Verificar se existem se a U/E/O tem normalizado procedimentos relativos à atribuição de classificação, reclassificação ou à desclassificação.

Av: P: 3**C1.2 - Reprodução, Transferência, Registo e Controlo de Segurança, Destruição e Evacuação da IC**P: 1

1 - Verificar se existem máquinas fotocopadoras disponíveis em áreas abertas (i.e.: salas abertas, corredores). Em caso afirmativo, o acesso é controlado (i.e.: por meio de cartão / código de acesso ou outro).

Av: P: 3

2 - Verificar se são cumpridos os procedimentos de transferência da IC e são elaborados registos de transferência, de acordo com o grau de classificação de segurança dos documentos.

Av: P: 3

3 - Verificar se a transferência interna da IC (na U/E/O) é transportada por pessoal devidamente credenciado e protegida de modo a não permitir a observação do seu conteúdo.

Av: P: 3

4 - Verificar se a transmissão da IC de grau RESERVADO, equivalente ou superior, é efetuada através de circuitos protegidos por produtos criptográficos aprovados.

Av: P: 3

5 - Verificar se são mantidos os registos de controlo apropriados dos documentos classificados NATO SECRET / SECRET UE/ SECRETO (Registo, recibo, certificados de destruição, retenção de registos de controlo).

Av: P: 2

6 - Verificar se os documentos NATO SECRET / SECRET UE / SECRETO são sujeitos a verificações periódicas e são mantidos os registos.

Av: P: 2

7 - Verificar se existe lista de acesso a informação classificada com o grau de SECRETO, equivalente e superior.

Av: P: 2

8 - Verificar se existe controlo para documentos NATO CONFIDENTIAL, CONFIDENTIEL UE, CONFIDENCIAL e equivalentes.

Av: P: 2

9 - Verificar se existem procedimentos / equipamentos aprovados para a destruição dos documentos classificados.

Av: P: 2

10 - Verificar se existe uma revisão sistemática / programa dos documentos, com vista à destruição dos que já não são necessários.

Av: P: 2

11 - Verificar se os documentos classificados são destruídos da forma correta.

Av: P: 3

12 - Verificar se os certificados de destruição são retidos, pelo menos, durante 5 anos para os graus SECRETO / CONFIDENCIAL ou equivalentes.

Av: P: 2

13 - Verificar se existe um plano de destruição de IC e cumpre os requisitos necessários conforme normativo em referência.

Av: P: 3

14 - Verificar se existe um plano de evacuação de emergência da IC e cumpre os requisitos necessários conforme normativo em referência.

Av: P: 3

D - SEGURANÇA DO PESSOALP: 1**D1 - MEDIDAS DE SEGURANÇA MILITAR COM PESSOAL**P: 1**D1.1 - Credenciação de Segurança Pessoal**P: 1

1 - Verificar se existem listas de acesso, individualizadas, para cada grau de classificação (Mod. G-7, G-8 e G-9) onde seja manuseada IC com os graus de MUITO SECRETO, SECRETO e CONFIDENCIAL.

Av: P: 2

2 - Verificar que as U/E/O que detenham IC asseguram que todos os militares, militarizados e civis a quem tal informação tenha de ser confiada estão credenciados para o seu manuseamento.

Av: P: 3

3 - Verificar se os quarteleiros estão credenciados.

Av: P: 3

4 - Verificar se o OfSegCSI está adequadamente credenciado.

Av: P: 3

5 - Verificar se todo o pessoal do Centro de Comunicações (CCom) está adequadamente credenciado.

Av: P: 3

6 - Verificar se o Administrador de Rede Local está adequadamente credenciado.

Av: P: 2

7 - Verificar se o Custódio Cripto, Custódio Cripto Substituto e eventuais Operadores Cripto estão credenciados com o designador Cripto.

Av: P: 3

8 - Verificar se as empresas prestadoras de serviços nas Áreas de Segurança (Classe I e II) e Restritas (AMG e PAIOL), estão credenciadas, bem como os seus colaboradores.

Av: P: 3

9 - Verificar se a U/E/O cumpre os procedimentos necessários com os prestadores de serviços.

Av: P: 3

10 - Verificar se estão identificados os procedimentos de credenciação de segurança do pessoal, de acordo com os requisitos Nacional/NATO/UE.

Av: P: 3

11 - Verificar se estão estabelecidos procedimentos claros de renovação com a antecedência necessária evitando a expiração da credenciação de segurança, caso se verifique essa necessidade.

Av: P: 3

12 - Verificar se a U/E/O mantém os registos atualizados das CSP, nos quais devem constar o grau de classificação de segurança, a data e a validade.

Av: P: 2

13 - Verificar se os correios, guardas e escoltas utilizados no transporte da IC de grau CONFIDENCIAL e superior são credenciados no mesmo grau da IC que transportam, são instruídos sobre os deveres para proteção da IC que lhes é confiada, assim como dos procedimentos de segurança a aplicar, nomeadamente, o plano de destruição da mesma na iminência da sua passagem para pessoal não autorizado.

Av: P: 2

14 - Verificar se existe acesso excecional a IC e um registo das pessoas a quem tenha sido concedido este acesso.

Av: P: 2**D1.2 - Formação em Segurança Militar**P: 1

1 - Verificar se existem quebras de segurança e se foram inseridas no Programa de Educação e Consciencialização em Segurança Militar (PECSM) a título de exemplo.

Av: P: 3

2 - Verificar se a U/E/O tem o seu PECSM instituído, abrangendo todo o militar, militarizado ou civil que inicia funções, que permanece em funções e após deixar as fileiras ou cessar as suas funções em que tenham tido acesso privilegiado a IC.

Av: P: 3

3 - Verificar se os briefing(s) de segurança à chegada dos militares abrangem todas as áreas de segurança (Física, Informação, Pessoal e SIC).

Av: P: 3

4 - Verificar se existe um registo para controlo de presenças nos brifingues (iniciais de acompanhamento e cessação de funções).

Av: P: 3

5 - Verificar se todo o pessoal que desempenha funções afetas à SEGMIL na U/E/O está habilitado com curso de SEGMIL, ou equivalente.

Av: P: 3**D1.3 - Controlo de Drogas e Álcool**P: 1

1 - Verificar se estão identificados e são executados os procedimentos a adotar nos rastreios toxicológicos, ao álcool e cinotécnicas.

Av: P: 2

2 - Verificar se a U/E/O realiza atividades no âmbito da dissuasão e deteção do consumo de álcool e drogas, ou posse de substâncias ilícitas, através dos diferentes rastreios definidos no documento em referência.

Av: P: 3

3 - Verificar se existe a nomeação e funcionamento do Núcleo de Apoio ao Comando (NAC)

Av: P: 2

4 - Verificar se os elementos do NAC estão habilitados com o Curso de Operadores de Prevenção de Comportamentos Aditivos e Dependência (COPCAD).

Av:

P:

5 - Verificar se são realizadas Ações de Informação e Esclarecimento (AIE) pelo NAC.

Av:

P:

E - SEGURANÇA CSI		P:	<input type="text" value="1"/>
E1 - PESSOAL		P:	<input type="text" value="1"/>
E1.1 - Habilitações do Pessoal de Segurança das CSI		P:	<input type="text" value="1"/>
1 - Verificar se o Oficial de Segurança das CSI (OfSegCSI)/Oficial de Segurança Local SIC (OSLSIC) está habilitado com formação adequada, nomeadamente com o Curso de Transmissões das Armas.	Av: <input type="text"/>	P:	<input type="text" value="1"/>
2 - Verificar se o Administrador de Rede Local (ARL) está habilitado com conhecimentos técnicos de administração e segurança de redes.	Av: <input type="text"/>	P:	<input type="text" value="3"/>
3 - Verificar se Custódio Cripto está habilitado com o Curso de Material e Segurança Cripto.	Av: <input type="text"/>	P:	<input type="text" value="3"/>
4 - Verificar se o Custódio Cripto Substituto está habilitado com o Curso de Material e Segurança Cripto.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
5 - Verificar se os operadores do Centro Cripto (CCp) estão habilitados com o Curso de Material e Segurança Cripto.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
E2 - SEGURANÇA DAS COMUNICAÇÕES		P:	<input type="text" value="1"/>
E2.1 - Rede Local de Comunicações		P:	<input type="text" value="1"/>
1 - Rede Local do Domínio Classificado (Rede Red): verificar se o que está instalado na U/E/O corresponde ao cadastro autorizado.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
2 - No âmbito da Rede Local do Domínio Classificado, verificar que não existe alguma infraestrutura/equipamentos/dispositivos CSI não autorizados que possam interferir com as CSI autorizadas. Caso existam, devem ser identificados	Av: <input type="text"/>	P:	<input type="text" value="3"/>
3 - Verificar se a Rede do Domínio Classificado (Rede Red) quando atravessa áreas de classe de segurança inferiores (Classe 3 ou Área administrativa) cumpre os requisitos mínimos de segurança estabelecidos para a implementação da infraestrutura de rede e instalação de equipamentos.	Av: <input type="text"/>	P:	<input type="text" value="3"/>
4 - Verificar se o ARL tem um cadastro atualizado das ligações físicas e lógicas de todos os equipamentos de rede existentes na U/E/O.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
5 - Verificar se o ARL dispõe de material essencial necessário para o bom desempenho das funções.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
6 - Verificar se existe alguma infraestrutura/equipamentos/dispositivos CSI não autorizados que possam interferir com as CSI autorizadas.	Av: <input type="text"/>	P:	<input type="text" value="3"/>
E2.2 - Sala Técnica CSI (Verificar se nas Áreas Críticas CSI, os sistemas de segurança eletrónicos cumprem os requisitos definidos no SICAVE para áreas de segurança CI 1)		P:	<input type="text" value="1"/>
1 - Verificar se a pintura interior está em bom estado de conservação.	Av: <input type="text"/>	P:	<input type="text" value="1"/>
2 - Verificar se está limpo e arrumado.	Av: <input type="text"/>	P:	<input type="text" value="1"/>
3 - Verificar se existe um Registo de Visitas para pessoal não autorizado com necessidade de aceder às áreas críticas (ex: ações de manutenção).	Av: <input type="text"/>	P:	<input type="text" value="1"/>
4 - Verificar se o sistema de climatização da Sala Técnica CSI da U/E/O se encontra operacional.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
5 - Verificar se a Sala Técnica CSI da U/E/O tem implementados sistema de energia socorrida (Grupo Gerador) e/ou sistema de energia permanente (UPS) e que estejam operacionais.	Av: <input type="text"/>	P:	<input type="text" value="2"/>
6 - Existe a devida separação nos bastidores entre os equipamentos RED/BLACK (se possível, existência de bastidores RED e BLACK).	Av: <input type="text"/>	P:	<input type="text" value="2"/>
7 - Verificar a existência de chaveiro com coleção de chaves, devidamente identificadas, dos bastidores e salas de alojamento dos equipamentos CSI.	Av: <input type="text"/>	P:	<input type="text" value="3"/>
8 - Verificar se o ARL têm conhecimento mínimo de todo o equipamento existente na sala técnica.	Av: <input type="text"/>	P:	<input type="text" value="1"/>
E2.3 - Equipamentos CSI		P:	<input type="text" value="1"/>
1 - Verificar se os selos de segurança não instalados e/ou violados dos equipamentos ativos e passivos CSI que processam IC estão justificados pelo OfSegCSI.	Av: <input type="text"/>	P:	<input type="text" value="3"/>

2 - Verificar a existência de chaveiro com coleção de chaves devidamente identificadas das salas técnicas e dos bastidores dos equipamentos CSI. Av: P: 1

E2.4 - Equipamentos Criptográficos

P: 1

1 - Verificar se os selos de segurança não instalados e/ou violados dos equipamentos Criptográficos estão justificados pelo OfSegCSI. Av: P: 3

2 - Verificar se a lista de equipamentos criptográficos existente na U/E/O está de acordo com as existências. Av: P: 3

E2.5 - Documentação Interna

P: 1

1 - Verificar se existem NEP's CSI. Av: P: 1

2 - Verificar se as NEP's CSI estão atualizadas de acordo com as NAT da DCI e diretivas superiores. Av: P: 2

3 - Verificar se existe Anexo de Transmissões e ITTm ao Plano de Segurança e que é adequado. Av: P: 2

4 - Verificar se existe e se é do conhecimento dos Custódios Cripto a documentação relativa ao controlo e distribuição de material cripto. Av: P: 2

5 - Verificar que os Procedimentos de Operação de Segurança (SecOPs) do Domínio Classificado da Rede de Dados do Exército (DClas-RDE) são do conhecimento de todos os utilizadores deste domínio. Av: P: 3

E3 - CENTRO DE COMUNICAÇÕES (CCom) (Área de Segurança Classe 1)

P: 1

E3.1 - Segurança Física do Centro de Comunicações

P: 1

1 - Verificar se a construção da estrutura e sólida, nomeadamente: betão, tijolo ou material equivalente. Av: P: 3

2 - Verificar se a porta de acesso exterior cumpre com os requisitos apropriados. Av: P: 3

3 - Se existir porta exclusivamente como saída de emergência. Caso exista, não permite a sua abertura a partir do exterior. Av: P: 3

4 - Verificar se o sistema de abertura elétrico, utilizado no controlo de acessos, é no mínimo de resistência de 500 Kg-f. Av: P: 3

5 - Verificar se todas as janelas e outras aberturas situadas a menos de 5,5 metros de altura do solo, nomeadamente tetos/telhados, lajes, parapeitos ou tubos de drenagem de águas pluviais estão protegidas conforme as ISM. Av: P: 3

6 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência, se aplicável e emite os alertas na sala do SICAVE. Av: P: 3

7 - Verificar se existe sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna. Av: P: 3

8 - Verificar se existe um sistema de controlo de entradas por dupla autenticação, nomeadamente, cartão eletrónico e PIN ou sistema de leitura biométrica. Av: P: 3

9 - Verificar se está afixada no seu interior, uma lista de acessos permanentes autorizados àquela área, devendo os movimentos de todas as pessoas que não constarem da referida lista, ser registados e assinados. Av: P: 3

10 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma. Av: P: 2

11 - Verificar se existe identificação de Área de Segurança de Classe 1 e painéis informativos de entrada em Áreas de Segurança, na porta ou na parede. Av: P: 1

E3.2 - Material e Equipamento do Centro de Comunicações

P: 1

1 - Verificar se existe contentor de segurança Classe B com fechadura grupo A ou B. Av: P: 3

2 - Verificar se existe contentor de segurança Classe C com sistema de fecho do grupo B ou C. Av: P: 2

3 - Verificar se os únicos detentores do segredo das combinações das fechaduras do Grupo A e B são o Chefe e o Adjunto do CCp. Av: P: 2

4 - Verificar se as mudanças de combinações têm sido feitas com a seguinte periodicidade: # Quando da receção do dispositivo de segredo do fornecedor. # No mínimo, todos os 6 meses. # Sempre que haja mudança de pessoal com conhecimento dos mesmos. # Quando se tenha verificado qualquer quebra de segurança ou se suspeite dessa possibilidade.	Av: <input type="text"/>	P: <input type="text"/>	2
5 - Verificar se as mudanças de combinações são efetuadas apenas pelo Chefe e/ou Adjunto do CCom.	Av: <input type="text"/>	P: <input type="text"/>	2
6 - Verificar se existe uma cópia das combinações com o Oficial de Segurança da U/E/O em envelope fechado e lacrado.	Av: <input type="text"/>	P: <input type="text"/>	2
7 - Verificar se existe em funcionamento um dispositivo de destruição de documentos com IC.	Av: <input type="text"/>	P: <input type="text"/>	2
8 - Verificar se a marcação da classificação de segurança dos equipamentos CSI em produção no CCom está de acordo com o mais elevado grau de classificação de segurança da IC que o equipamento processa ou tenha processado.	Av: <input type="text"/>	P: <input type="text"/>	2

E4 - CENTRO CRIPTO (CCp) (Área de Segurança – Classe 1)

P: 1

E4.1 - Segurança Física do CCp

P: 1

1 - Verificar se a construção da estrutura é sólida, nomeadamente: betão, tijolo ou material equivalente.	Av: <input type="text"/>	P: <input type="text"/>	3
2 - Verificar se a porta de acesso exterior cumpre com os requisitos apropriados.	Av: <input type="text"/>	P: <input type="text"/>	3
3 - Se existir porta exclusivamente como saída de emergência. Caso exista, não permite a sua abertura a partir do exterior.	Av: <input type="text"/>	P: <input type="text"/>	3
4 - Verificar se o sistema de abertura elétrico, utilizado no controlo de acessos, é no mínimo de resistência de 500 Kg-f.	Av: <input type="text"/>	P: <input type="text"/>	3
5 - Verificar se todas as janelas e outras aberturas situadas a menos de 5,5 metros de altura do solo, nomeadamente tetos/telhados, lajes, parapeitos ou tubos de drenagem de águas pluviais estão protegidas conforme as ISM.	Av: <input type="text"/>	P: <input type="text"/>	3
6 - Verificar se existe alarme de intrusão cobrindo os acessos à área pela porta principal e de emergência, se aplicável e emite os alertas na sala do SICAVE.	Av: <input type="text"/>	P: <input type="text"/>	3
7 - Verificar se existe sistema de VV a cobrir a entrada da área a partir do exterior e permite a identificação clara da pessoa que acede e com capacidade de visualização diurna e noturna.	Av: <input type="text"/>	P: <input type="text"/>	3
8 - Verificar se existe um sistema de controlo de entradas por dupla autenticação, nomeadamente, cartão eletrónico e PIN ou sistema de leitura biométrica.	Av: <input type="text"/>	P: <input type="text"/>	3
9 - Verificar se está afixada no seu interior, uma lista de acessos permanentes autorizados àquela área, devendo os movimentos de todas as pessoas que não constarem da referida lista, ser registados e assinados.	Av: <input type="text"/>	P: <input type="text"/>	3
10 - Verificar se existe iluminação de segurança que, em conjunto com o sistema de VV instalado, permita a identificação facial de quem entra ou sai da mesma.	Av: <input type="text"/>	P: <input type="text"/>	2
11 - Verificar se existe identificação de Área de Segurança de Classe 1 e painéis informativos de entrada em Áreas de Segurança, na porta ou na parede.	Av: <input type="text"/>	P: <input type="text"/>	1

E4.2 - Portas de Acesso e Fechaduras (sem CA electrónico implementado)

P: 1

1 - Verificar se existe uma relação das chaves existentes.	Av: <input type="text"/>	P: <input type="text"/>	2
2 - Verificar se existe uma cópia das chaves com o Oficial de Segurança/Claviculario da U/E/O em envelope fechado e lacrado.	Av: <input type="text"/>	P: <input type="text"/>	3
3 - Verificar se os únicos detentores do segredo da combinação da fechadura da porta de entrada são o Custódio Material Cripto e o Adjunto do Custódio material Cripto.	Av: <input type="text"/>	P: <input type="text"/>	3
4 - Verificar se as mudanças de combinações têm sido feitas com a seguinte periodicidade: # Quando da receção do dispositivo de segredo do fornecedor. # No mínimo, todos os 6 meses. # Sempre que haja mudança de pessoal com conhecimento dos mesmos. # Quando se tenha verificado qualquer quebra de segurança ou se suspeite dessa possibilidade.	Av: <input type="text"/>	P: <input type="text"/>	3
5 - Verificar se existe uma cópia das combinações com o Oficial de Segurança da U/E/O em envelope fechado e lacrado.	Av: <input type="text"/>	P: <input type="text"/>	3

E4.3 - Material e equipamentos do CCpP:

1 - Verificar se a marcação da classificação de segurança dos equipamentos CSI está de acordo com o mais elevado grau de classificação de segurança da IC que o equipamento processa ou tenha processado.

Av: P:

3 - Verificar que não existem dispositivos de VV instalados no interior do CCp.

Av: P:

4 - Verificar que não existem dispositivos de comunicação móvel no interior do CCp.

Av: P:

5 - Verificar que não existem telefones sem fios ou outros equipamentos radiantes no interior do CCp.

Av: P:

6 - Verificar se existe contentor de segurança Classe B com fechadura grupo A ou B.

Av: P:

7 - Verificar se os Certificados de Posse (CP) de material cripto existem e estão corretos.

Av: P:

8 - Verificar se os Certificados de Transferência (CT) de material cripto estão corretos.

Av: P:

9 - Verificar se os Certificados de Destruição (CD) de material cripto estão corretos.

Av: P:

10 - Verificar se os documentos/material cripto estão separados pela sua situação: em Vigor, em Reserva e a Aguardar Destruição.

Av: P:

11 - Verificar se os documentos/material cripto de destruição periódica foram destruídos nas datas previstas.

Av: P:

12 - Verificar se os documentos/material cripto que devem ser do conhecimento do Comando têm o respetivo VISTO.

Av: P: **E4.4 - Planos de Segurança**P:

1 - Verificar se está elaborado um Plano de Evacuação de Emergência do CCp.

Av: P:

2 - Verificar se está elaborado um Plano de Destruição de Emergência de documentos/material do CCp.

Av: P:

3 - Verificar se o local de alternativa está previsto nos planos e se é exequível.

Av: P:

4 - Verificar se está elaborado um Plano Contra Incêndios no CCp e integrado no restante plano da U/E/O.

Av: P:

5 - Verificar se os planos estão aprovados pelo Comando da U/E/O.

Av: P: **E4.5 - Controlo do Encerramento**P:

1 - Verificar se existe, junto à porta de entrada, a lista de verificação regulamentar.

Av: P:

2 - Verificar se o controlo de encerramento é feito corretamente pelos responsáveis.

Av: P: **E5 - SEGURANÇA DOS COMPUTADORES(COMPUSEC)**P: **E5.1 - Formação e Procedimentos**P:

1 - Verificar se a U/E/O tem difundido as normas técnicas e sensibilizado de forma permanente os utilizadores para os aspetos de segurança da informação e de operação dos e sistemas de informação:

Cuidados com o equipamento, manuseamento de matérias classificadas, políticas de segurança e sistema de relato de incidentes.

Av: P:

2 - Verificar se existe um cadastro atualizado de todos os equipamentos e sistemas de informação adicionados ao domínio exercito.local na organization unit (OU) da U/E/O.

Av: P:

3 - Nos equipamentos que processam IC, verificar se os utilizadores com registos de acesso ao equipamento possuem a credenciação adequada.

Av: P:

4 - Verificar se o ARL tem uma relação exata de todos os utilizadores que pertencem a cada grupo de segurança e se esta é a adequada às funções desempenhadas.

Av: P:

5 - Verificar se a U/E/O tem procedimentos definidos para efetuar cópias de segurança (backups).

Av: P: **E5.2 - Informação Processada na RDE**P:

1 - Verificar se no caso de matérias classificadas acima de RESERVADO são cumpridos os termos do Despacho de 25Mar04, de SEEx. o General CEME.

Av: P:

2 - Verificar se a marcação da classificação de segurança de todos os equipamentos CSI de armazenamento e de impressão está efetuada.

Av: P:

3 - Verificar se existem acessos a conteúdos não autorizados da internet.

Av: P:

4 - Verificar se apenas software oficialmente obtido e licenciado é utilizado nos computadores/estações de trabalho da U/E/O.

Av: P: