

Domínio Classificado da Rede de Dados do Exército (DCIas-RDE)

PROCEDIMENTOS DE OPERAÇÃO DE SEGURANÇA (SecOPs)

Versão 1.0

Março de 2024

Página intencionalmente em branco

Procedimentos de Operação de Segurança (SecOPs)

DOMÍNIO CLASSIFICADO DA REDE DE DADOS DO EXÉRCITO

Direção de Comunicações e Informação, Exército Português

Versão 1.0, 20 de março de 2024

Página intencionalmente em branco



MINISTÉRIO DA DEFESA NACIONAL
EXÉRCITO PORTUGUÊS
VICE-CHEFE DO ESTADO-MAIOR DO EXÉRCITO
DIREÇÃO DE COMUNICAÇÕES E INFORMAÇÃO
DESPACHO

1. Aprovo, ao abrigo do Despacho n.º 11572/2023 do Vice-Chefe do Estado-Maior do Exército de 19 de setembro de 2023, para utilização no Exército, os Procedimentos de Operação de Segurança (*Security Operating Procedures* – SecOPs) do Domínio Classificado da Rede de Dados do Exército (DClas-RDE).
2. Estes SecOPs constituem-se como uma versão provisória que deverá ser submetida posteriormente à Autoridade Nacional de Segurança aquando do processo de acreditação da rede.
3. Os SecOPs DClas-RDE são uma publicação classificada de RESERVADO.
4. Podem ser feitos extratos desta publicação sem autorização da entidade promulgadora, desde que sejam cumpridas as normas de tratamento de informação classificada.
5. Os SecOPs DClas-RDE entram em vigor a partir da data da sua aprovação.

Lisboa, 20 de março de 2024

O DIRETOR DA DCI

Rui Jorge Fernandes Bettencourt
Cor Tir Tm

Página intencionalmente em branco

Índice

Referências	8
Lista de Abreviaturas e Acrónimos.....	9
1. Introdução.....	11
2. Administração da Segurança	12
Anexo A – SecOPs para Utilizadores	17
A.1. Introdução e Organização da Segurança.....	17
A.2. Segurança Física	19
A.3. Segurança do Pessoal	19
A.4. Segurança da Informação classificada.....	21
A.5. Segurança do SIC.....	24
A.6. Segurança da Emissão	26
A.7. Violações de Segurança	26
A.8. Plano de Contingência do Utilizador.....	27
Anexo B – SecOPs para Administradores	29
B.1. Introdução.....	29
B.2. Administração e Organização de Segurança	29
B.3. Segurança Física	32
B.4. Segurança do Pessoal	33
B.5. Segurança da Informação Classificada.....	35
B.6. Segurança SIC	35
B.7. Gestão da Segurança e Auditoria	39
B.8. Segurança Criptográfica	39
B.9. Segurança da Emissão	39
B.10. Plano de Emergência	40
Anexo C – Formulário de Pedido de Acesso	43
Anexo D – <i>Brifingue</i> de Segurança.....	45
Anexo E - Declaração de Conhecimento dos SecOPs	47
Anexo F – Formulário de Relatório de Incidente de Segurança.....	49
Anexo G – Formulário de Pedido de Alteração de Configuração.....	51
Anexo H – Formulário de Pedido de Gravação de Dados.....	55
Anexo I – Controlo das Impressões em Papel	57
Anexo J – Administração da Segurança: Listagem de Pontos de Contacto	59
Anexo K – Registo de Alterações dos SecOPs.....	61

Referências

[ISM]

Instruções de Segurança Militar, 2020

[NT GNS]

Normas Técnicas do Gabinete Nacional de Segurança

[PAD 320-01]

Normas de elaboração de publicações do Exército

Documentação da NATO

[C-M(2002)49]

Security Within the North Atlantic Treaty Organization

[AC/35-D/2004]

Primary Directive on CIS Security

[AC/322-D/0048]

Technical and Implementation Directive on CIS Security

[AC/35-D/1014]

Guidelines for the Structure and Content of Security Operating Procedures (SecOPs) for Communications and Information Systems (CIS)

[AC/322-D(2007)0036]

INFOSEC Technical and Implementation Directive on Emission Security

[SDIP-28]

NATO Zoning Procedures

[SDIP-29]

SDIP-29/1 Facility Design Criteria and Installation of Equipment for the Processing of Classified Information;

[SDIP-293]

SDIP-293/1 Instruction for the Control and Safeguarding of NATO Cryptomaterial

Documentos específicos do sistema (ainda em elaboração)

[DCLAS-RDE - Descrição do SIC]

Descrição do Sistema DCLAS-RDE (*versão e data TBD*)

[PRT CHOD SECNET CSRS]

Community Security Requirement Statement (CSRS) for PRT OPNET (*versão e data TBD*)

[DCLAS-RDE - SRA]

Avaliação de Risco de Segurança (ARS) para DCLAS-RDE (*versão e data TBD*)

[DCLAS-RDE - SSRS]

Declaração de Requisitos de Segurança Específicos do Sistema (SSRS) do DClas (*versão e data TBD*)

[DCLAS-RDE - STVP]

Teste de Segurança e o Plano de Verificação do DClas (*versão e data TBD*)

Lista de Abreviaturas e Acrónimos

ANS	Autoridade Nacional de Segurança
ARL	Administrador de Rede Local
CFT	Comando das Forças Terrestres
CGIC	Centro de Guerra de Informação e Ciberespaço
CIS	<i>Communications and Information Systems</i> , é o mesmo que SIC
CISOA	<i>CIS Operational Authority</i> / Autoridade Operacional do SIC
CISP	<i>Communications and Information Systems Provider</i> / Fornecedor do Sistema de Informação e Comunicações
CISPIA	<i>Communications and Information Systems Planning and Implementation Authority</i> / Autoridade de Planeamento e Implementação do SIC
CISSEO	<i>CIS Security Officer</i> / Oficial de Segurança do SIC
COMPUSEC	<i>Computer Security</i> / Segurança dos Computadores
COMSEC	<i>Communications Security</i> / Segurança das Comunicações
CSP	Credenciação de Segurança Pessoal
CSRS	<i>Community Security Requirement Statement</i> / Declaração de Requisitos de Segurança da Comunidade
CTE	Centro de Transmissões do Exército
DCI	Direção de Comunicações e Informação
EMGFA	Estado-Maior-General das Forças Armadas
EMSEC	<i>Emission Security</i> / Segurança das Emissões
ISM	Instruções de Segurança Militar
LCISSEO	<i>Local CIS Security Officer</i> / Oficial de Segurança Local do SIC - é o mesmo que OfSegCSI
LSA	<i>Local System Administrator</i> / Administrador Local do Sistema – é o mesmo que ARL
OfSegCSI	Oficial de Segurança das Comunicações e Sistemas de Informação
SA	<i>System Administrator</i> / Administrador do Sistema
SAA	<i>Security Accreditation Authority</i> / Autoridade de Acreditação de Segurança
SAP	<i>Security Accreditation Plan</i> / Plano de Acreditação de Segurança

SecOPs	<i>Security Operating Procedures</i> / Procedimentos de Operação de Segurança
SIC	Sistema de Informação de Comunicações
SRA	<i>Security Risk Assessment</i> / Avaliação de Riscos de Segurança
SRS	<i>Security Requirement Statement</i> / Declaração de Requisitos de Segurança
STVP	<i>Security Test & Verification Plan</i> / Teste de Segurança e o Plano de Verificação
U/E/O	Unidade/Estabelecimento/Órgão

1. Introdução

Este documento apresenta os Procedimentos de Operação de Segurança (SecOPs) do Domínio Classificado (DClas) da Rede de Dados do Exército (RDE), componente da infraestrutura do Sistema de Informação e Comunicações (SIC) do Exército.

Os SecOPs foram elaborados de acordo com as Instruções de Segurança Militar (Ref. [ISM]), tendo também em consideração os requisitos da Política de Segurança da NATO (Ref. [C-M (2002)49]) e outros documentos associados.

O DClas-RDE está ligado à rede “PRT OPNET” do Estado-Maior-General das Forças Armadas (EMGFA), pelo que o conteúdo destes SecOPs necessita de estar alinhado com a Declaração de Requisitos de Segurança da Comunidade (CSRS) do EMGFA (documento este ainda em modo de rascunho).

A estrutura do documento segue as orientações sobre o desenvolvimento de SecOPs (Ref. [AC/35-D/1014]) e está dividido nas seguintes partes:

- Anexo A – SecOPs para Utilizadores;
- Anexo B – SecOPs para Administradores;
- Anexo C – Formulário de Pedido de Acesso;
- Anexo D – Brífingue de Segurança;
- Anexo E – Declaração de Conhecimento dos SecOPs;
- Anexo F – Formulário de Relato de Incidente de Segurança;
- Anexo G – Formulário de Pedido de Alteração de Configuração;
- Anexo H – Formulário de Pedido de Gravação de Dados;
- Anexo I – Controlo das Impressões em Papel;
- Anexo J – Administração da Segurança: Lista de Pontos de Contacto;
- Anexo K – Registo de Alterações dos SecOPs;

Por norma, a uma unidade/estabelecimento/órgão (U/E/O) corresponde um *site* do DClas-RDE, doravante designado neste documento por DClas. Em cada *site*, os SecOPs devem ser adaptados/reajustados às necessidades reais de cada local e alterados, sempre que necessário, para acomodar procedimentos específicos de subsistemas. Contudo, se adaptados por *site*, deverão ser aprovados pela Autoridade Operacional do SIC.

2. Administração da Segurança

As responsabilidades específicas de segurança do SIC objeto deste documento, são atribuídas aos intervenientes enumerados seguidamente, de acordo com as responsabilidades gerais descritas nos documentos em referência.

2.1. Autoridade de Acreditação de Segurança

A Autoridade de Acreditação de Segurança (*Security Accreditation Authority* - SAA) reside na Autoridade Nacional de Segurança (ANS), que é Diretor-geral do Gabinete Nacional de Segurança (GNS), competindo-lhe coordenar e aprovar os processos de aprovação ou acreditação de segurança dos SIC das Forças Armadas. Tem a autoridade e a responsabilidade de regulamentação da generalidade dos aspetos para a área da segurança, incluindo os específicos do sistema.

2.2. Autoridade de Planeamento e Implementação do SIC

A Autoridade de Planeamento e Implementação do SIC (*Communications and Information Systems Planning and Implementation Authority* – CISPIA) cabe ao Vice-Chefe do Estado-Maior do Exército (VCEME), sendo encarregue da sua execução a Direção de Comunicações e Informação (DCI), que coopera em todo o processo de acreditação e re-acreditação e executa o planeamento e gestão do processo de implementação. Adicionalmente, é responsável pela formulação, promulgação e coordenação de todas as políticas e regulamentos de segurança administrativa e física para o DCIas.

2.3. Autoridade Operacional do SIC

A Autoridade Operacional do SIC (*CIS Operational Authority* – CISOA) reside no Comando das Forças Terrestres (CFT), sendo este comando responsável pela operação, garantindo a obtenção e manutenção de um nível adequado de proteção da Informação Classificada aí manuseada. É ainda responsável pela formulação, promulgação e coordenação de todos os aspetos de segurança militar relativamente ao DCIas.

2.4. Fornecedor do SIC

A tarefa de se constituir como Fornecedor do SIC (*Communications and Information Systems Provider* - CISP) cabe à DCI através do Centro de Guerra de Informação e Ciberespaço (CGIC) e do Centro de Transmissões do Exército (CTE), sendo estes órgãos responsáveis pela instalação, configuração, controlo de alterações e gestão em todo o seu ciclo de vida, de modo a garantir que os objetivos de segurança são atingidos e mantidos.

Os elementos-chave em termos da execução que possuem responsabilidades num âmbito global do DCIas são:

- a. Do CTE, o Administrador do Sistema (*System Administrator – SA*), que é o responsável por todas as operações técnicas realizadas diariamente, mantendo a rede do DCIas operacional em conformidade com as orientações recebidas;
- b. Do CGIC, o Oficial de Segurança do SIC (*CIS Security Officer – CISSO*), que é o responsável pela segurança do sistema, nomeadamente por garantir o adequado ambiente de segurança SIC e todos os aspetos lógicos/técnicos do DCIas.

2.5. Oficial de Segurança do SIC

O Oficial de Segurança do SIC (*CIS Security Officer – CISSO*) para o DCIas é o responsável pelos aspetos de segurança do sistema, auxiliado pelo Oficial de Segurança Local (*Local CIS Security Officer – LCISSO*) em cada site. Tem como deveres e responsabilidades específicas:

- a. Coordenar com o SA e com a autoridade de segurança física (os oficiais de segurança das U/E/O) todos os aspetos de segurança do SIC;
- b. Monitorizar atividades, deveres e responsabilidades relevantes para a segurança do administrador do Sistema;
- c. Definir os limites do ambiente de segurança eletrónica do DCIas e identifica áreas seguras;
- d. Monitorizar a implementação de alterações e melhorias de *hardware*, *firmware* e *software* para impedir a ocorrência de violações de segurança;
- e. Monitorizar os aspetos de controlo de configuração de alterações relacionadas com a segurança do *hardware*, *firmware* ou *software* e toda a documentação associada;
- f. Elaborar e manter atualizados os SecOPs do DCIas e efetuar a sua distribuição pelos destinatários tidos como necessários;
- g. Diligenciar para que seja garantida a sensibilização e formação necessária para os elementos com responsabilidades de segurança no DCIas;
- h. Manter um registo de todas as pessoas autorizadas a aceder aos terminais e serviços do DCIas;
- i. Manter um registo de auditoria com as atividades realizadas pelos utilizadores do DCIas, que permita em caso de necessidade a reconstrução de um histórico de eventos;
- j. Realizar inspeções de segurança aleatórias ao DCIas, efetuando o encaminhamento dos resultados da inspeção sob a forma de relatório, à CISOA;
- k. Realizar análises periódicas ao perfil de segurança do software em produção, interpretando o resultado e determinando alterações de segurança convenientes;

- l. Reportar à CISOA, sobre quaisquer deficiências e vulnerabilidades de segurança identificadas no DCIas;
- m. Conduzir inspeções inopinadas sobre possíveis violações de segurança do DCIas para determinar se investigações formais de segurança se justificam;
- n. Efetuar *site surveys* para análise do cumprimento dos requisitos de segurança, para a implementação de novos nós da rede;
- o. Prestar assistência técnica em investigações de possíveis violações de segurança no DCIas, em apoio ao CISSO;
- p. Manter a proficiência operacional do sistema do DCIas e do *software* de segurança implementado, a fim de monitorizar todas as atividades que possam constituir uma ameaça relevante para a segurança do DCIas;
- q. Auxiliar na elaboração e promulgação de SecOPs para novos locais onde a rede possa ser estendida.
- r. Atualização anual, ou sempre que existam mudanças de pontos de contacto, do Anexo J – Administração da Segurança: Listagem de Pontos de Contacto.

2.6. Administrador do Sistema

O Administrador do Sistema (*System Administrator* – SA) do DCIas é responsável pela administração "*hands-on*" do dia-a-dia, sendo auxiliado nos *sites* pelo Administrador do Sistema Local (*Local System Administrator* – LSA). Tem como deveres e responsabilidades específicas:

- a. Coordenar com o CISSO do DCIas todos os aspetos da segurança SIC do DCIas;
- b. Auxiliar o CISSO na definição dos limites do ambiente de segurança eletrónica do DCIas e na *compliance* das áreas seguras para implementação e extensão da rede;
- c. Implementar procedimentos de segurança no DCIas, em conformidade com as orientações do CISSO;
- d. Criar, manter e eliminar credenciais de utilizador do DCIas, com base em orientações do CISSO;
- e. Assegurar que todos os utilizadores do DCIas se encontram cientes das normas de segurança do DCIas e possuem a credenciação de segurança adequada;
- f. Implementar melhorias e as atualizações de *hardware*, *firmware* e *software* no DCIas necessárias a assegurar os níveis adequados de segurança do sistema;
- g. Assegurar que os registos de segurança do DCIas (i.e., registos de auditoria) são criados, gravados e arquivados;
- h. Garantir que a manutenção do DCIas é realizada sem a ocorrência de violações de segurança;

- i. Monitorizar *backups* efetuados e a recuperação de informação relevante sobre a segurança do sistema;
- j. Manter a proficiência do sistema operativo do DCIas e/ou *software* de segurança, a fim de implementar efetivamente todos os recursos relevantes para a segurança do DCIas;
- k. Verificar que os militares nomeados Administrador do Sistema Local (comummente designados de Administradores de Rede Local – ARL) nos diferentes *sites* locais têm a formação e os conhecimentos adequados para cumprimento das suas responsabilidades de administração do DCIas, assegurando, sempre que necessário, ações de esclarecimento e formação;
- l. Prestar assistência e apoio, sempre que requerido pelos Administradores de Rede Local nos *sites*;
- m. Fornecer contributos para a melhoria da segurança do sistema ao CISSO.

2.7. Administrador do Sistema Local

O Administrador do Sistema Local (*Local System Administrator* – LSA) do DCIas, é o também designado Administrador de Rede Local, nomeado pelo Comandante/Diretor/Chefe de cada U/E/O, é o responsável pela administração diária "*hands-on*" do *site* perante o utilizador final do DCIas. Tem como deveres e responsabilidades específicas:

- a. Coordenar com o SA do DCIas em todos os aspetos relativos à administração do DCIas
- b. Apoiar o SA na definição dos limites do ambiente de segurança eletrónica do DCIas e designar áreas seguras para implementação e extensão da rede;
- c. Implementar procedimentos de segurança do DCIas conforme orientações do SA;
- d. Receber pedidos para a criação, manutenção (incluindo atualização de data de término de credenciação após processo de renovação efetuado pelo utilizador/UEO) e eliminação de credenciais de utilizador do DCIas, de acordo com as orientações do LCISSE, submetendo esses pedidos ao SA;
- e. Assegurar que todos os utilizadores com acesso ao DCIas se encontram cientes das normas de segurança deste domínio de rede;
- f. Manter atualizada uma lista de todos os utilizadores autorizados no respetivo *site* do DCIas;
- g. Manter com frequência mensal um registo atualizado de todas as estações de trabalho do DCIas, especialmente no que respeita ao registo de *software* e *patches* de segurança, de acordo com as indicações do SA;
- h. Efetuar propostas de implementação de medidas de segurança adicionais, submetendo-as ao SA e LCISSE;

- i. Reportar ao SA e ao LCISSO qualquer incidente ou falha de *hardware/software*.

2.8. Oficial de Segurança Local do SIC

O Oficial de Segurança Local do SIC (*Local CIS Security Officer* – LCISSO), também designado por Oficial de Segurança das Comunicações e Sistemas de Informação (OfSegCSI), cumpre as suas funções de acordo com o definido no Regulamento Geral do Serviço nas Unidades, Estabelecimentos e Órgãos do Exército (RGSUE) e competências preconizadas nas ISM, coadjuvando o Oficial de Segurança da U/E/O na sua área específica, sendo responsável por todos os aspetos e elementos, relacionados com o ambiente de segurança global e os aspetos de segurança física do ambiente de segurança local das infraestruturas e equipamentos do DCIas. Tem como deveres e responsabilidades específicas:

- a. Coordenar com o CISSO do DCIas na definição dos limites do ambiente de segurança global e local do DCIas e a designação de áreas de segurança;
- b. Implementar procedimentos de segurança relativos ao ambiente de segurança global e local nas infraestruturas do DCIas em coordenação com o CISSO;
- c. Garantir a gestão dos elementos do ambiente de segurança global e local por forma a garantir ao DCIas os níveis de segurança preconizados;
- d. Contribuir para o processo de acreditação e re-acreditação do DCIas;
- e. Colaborar na realização de inspeções aos elementos de segurança do ambiente de segurança global e local do DCIas, encaminhando os resultados sob a forma de relatório à CISOA;
- f. Participar conjuntamente com o CISSO, em todas as investigações conduzidas relativamente a supostas violações de segurança do DCIas;
- g. Efetuar *site surveys* para análise do cumprimento dos requisitos de segurança, para a implementação de novos nós/extensões da rede;
- h. Contribuir para a elaboração e promulgação dos SecOPs para áreas e locais físicos distintos;
- i. Reportar ao CISSO, quaisquer deficiências e vulnerabilidades de segurança do DCIas, que venham a ser identificadas em qualquer elemento do domínio de segurança do ambiente de segurança global e local;
- j. Gerir o controlo de acessos e manter um registo atualizado de todas os elementos autorizados a aceder às áreas de segurança afetas às infraestruturas do DCIas;

Anexo A – SecOPs para Utilizadores

Procedimentos Operacionais de Segurança (SecOPs) para Utilizadores do DCIas

A.1. Introdução e Organização da Segurança

Este anexo constitui os SecOPs do DCIas para UTILIZADORES, rede esta que permite armazenar, processar e transmitir informação classificada NACIONAL até e incluindo NACIONAL SECRETO.

Estes SecOPs são emitidos pela Autoridade de Planeamento e Implementação do SIC (CISPIA) de acordo com os requisitos contidos na legislação nacional e também em consonância com política de segurança da NATO [C-M(2002)49] e documentação associada.

Os pontos de contacto listados no anexo J, podem fornecer orientações em caso de dúvidas ou incidentes relacionados com segurança. A atualização da lista de pontos de contacto deve ser feita sempre que aconteçam mudanças dos responsáveis na administração e segurança do sistema.

A.1.1. Pontos de Contacto

A.1.1.1. *Service Desk*

Cabe ao CTE manter o canal de apoio (*Service Desk*) aos administradores do DCIas.
Ver Anexo J – Administração da Segurança: Listagem de Pontos de Contacto.

A.1.1.2. Administrador do Sistema (SA)

Cabe ao CTE nomear o Administrador do Sistema para o DCIas.
Ver o Anexo J – Administração da Segurança: Listagem de Pontos de Contacto.

A.1.1.3. Oficial de Segurança do SIC (CISSO)

Cabe ao CGIC nomear o Oficial de Segurança do SIC para o DCIas.
Ver o Anexo J – Administração da Segurança: Listagem de Pontos de Contacto.

A.1.2. Classificações de Segurança

O DCIas é aprovado para armazenamento, processamento e transmissão de informação classificada até e incluindo NACIONAL SECRETO.

A.1.3. Responsabilização dos utilizadores

Os utilizadores que necessitem de acesso ao DCIas deverão tomar conhecimento do presente documento e assinar o formulário que se constitui como anexo E.

A.1.4. Pedido de Acesso, Identificação e Autorização

O acesso ao DCIas só pode ser concedido aos utilizadores que completaram o processo de registo, não devendo ser permitido o acesso antes de ser recebida a respetiva aprovação.

O pedido de criação ou alteração de uma conta de utilizador do DCIas começa com o preenchimento do Formulário de Pedido de Acesso, Anexo C, juntamente com a assinatura do Anexo E.

O CISSO do DCIas, aprova todos os pedidos de credenciais de utilizador. Uma vez aprovada, a conta de utilizador e *password* inicial são geradas para o utilizador pelo SA/Service Desk. Nesse momento, são atribuídos os grupos e serviços que o utilizador estará autorizado a aceder. Os privilégios de acesso para funções de extração de dados da rede, deverão ser especificados pelo CISSO do DCIas.

O acesso do utilizador ao DCIas implica que este esteja credenciado em NACIONAL SECRETO, sendo que os *usernames*, deverão ser únicos. A partilha de credenciais de utilizador não é autorizada.

No primeiro *login*, é solicitado ao utilizador a alteração da sua *password* inicial. As *passwords* do utilizador devem ser únicas, não repetidas, conhecidas apenas pelo utilizador e não deverão ser anotadas. A *password* deve ter pelo menos 9 caracteres e exigem a inclusão de 3 dos 4 seguintes conjuntos de caracteres: letras minúsculas (a.. z), letras maiúsculas (A.. Z), numerais (0.. 9), e caracteres especiais (~ ! @ \$ % ^ & * _ | ' - = \ } < > [] . /). A *password* deve ser alterada a cada 90 dias, ou quando for comprometida ou se suspeite de ter sido comprometida. O recurso a *passwords* anteriores é igualmente negado.

As credenciais de utilizador serão automaticamente bloqueadas após três (3) tentativas de autenticação malsucedidas e bloqueadas manualmente se se suspeitar que a conta esteja a ser utilizada de forma incorreta. O desbloqueio de credenciais requer a intervenção do SA/Service Desk.

Credenciais que não sejam mais necessárias, deverão ser reportadas pelos LCISSO e serão bloqueadas ou eliminadas.

Credenciais específicas para efeitos de treino serão desativadas quando a sua utilização não se justificar (i.e., quando o treino não estiver a ser realizado).

O SA/Service Desk, deverá possuir uma lista de utilizadores autorizados.

As credenciais de utilizador e respetivas *passwords* são da responsabilidade exclusiva do utilizador, que deve tomar todas as precauções para evitar o acesso de terceiros.

Precauções específicas devem ser tomadas ao realizar o *login* (ou seja, certificar-se de que nenhuma pessoa está por perto para observar quais os caracteres digitados).

Os utilizadores não devem deixar a estação de trabalho com a sessão iniciada. Deverá estar definida a política de bloqueio de ecrã após 15 minutos sem interação.

O utilizador deve utilizar atalhos de teclado para criar esse bloqueio de ecrã manualmente, por exemplo, a tecla *Windows* juntamente com "L" (letra pequena "L") ou ALT, CTRL, DEL → *Lock* deste computador.

O utilizador, antes de sair do seu local de trabalho, deve bloquear o ecrã ou efetuar *log off* da sua sessão (se mais de 5 minutos). No final do dia de trabalho, deverá ser feito o *log off*.

O Sistema Operativo deve ser configurado para lembrar os utilizadores quando as *passwords* devem ser alteradas.

A.2. Segurança Física

O terminal do utilizador deve estar localizado numa Área de Segurança Classe 2 ou Classe 1 e a sua localização não deve ser alterada sem a devida autorização. O acesso de pessoal e equipamento deve ser controlado em conformidade com as instruções de segurança locais, nomeadamente no que diz respeito ao acompanhamento de visitantes, remoção de equipamentos, equipamentos periféricos não autorizados e *wearables*.

Os selos de segurança do *hardware* deverão ser verificados diariamente e os selos partidos devem ser reportados ao Administrador do Sistema/Oficial de Segurança.

Discos rígidos fixos classificados SECRETO necessitam de mecanismos de controlo de acordo com as políticas aprovadas e instruções de segurança locais.

A.3. Segurança do Pessoal

O acesso é concedido apenas a utilizadores que detêm credenciação de segurança pessoal válida (CSP) na marca NACIONAL com o grau de SECRETO.

A.3.1 Controlo de Visitantes

Todos os visitantes devem ser controlados à entrada. Um registo em papel deverá ser mantido na porta de entrada, onde deverá estar o registo de identificação, motivo da visita e quem irá receber o visitante. Todos os visitantes deverão estar permanentemente acompanhados, podendo ser alvo de inspeções inopinadas de segurança. O pessoal que acompanha os visitantes deve garantir que todos os monitores dos computadores estão bloqueados e que informação classificada não está visível.

Os registos de visitantes são mantidos em arquivo pelo menos seis (6) meses, devendo ser regularmente controlados.

A.3.2 Cartão de Identificação

Todos os militares/civis que trabalham dentro do designado ambiente de segurança local, normalmente uma Área de Segurança Classe 2, são identificados com cartões de identificação que devem ser utilizados permanentemente. Os cartões são emitidos pela estrutura de segurança da U/E/O.

A.3.3 Equipamento Diverso

Qualquer equipamento diverso que aceda ao ambiente de segurança local deverá ser submetido a uma inspeção de segurança prévia e carece de autorização do LCISSO por cada *site*.

Se for necessário o acesso aos equipamentos COMSEC deverão ser aplicados os procedimentos de controlo COMSEC (Ref. [SDIP-293]).

A.3.4 Pessoal Autorizado

A entrada e o acesso não acompanhado aos locais onde está instalado o DCIas, incluindo áreas onde se localizam as estações de trabalho, limita-se a militares/civis com a credenciação adequada. Os militares/civis são credenciados pelo menos para o nível mais elevado e para as marcas da categoria de informação às quais suas funções lhes possam dar acesso.

A.3.5 Pessoal Essencial Autorizado

Uma lista de todos os militares e civis autorizados, deverá ser mantida por cada *site* pelo Oficial de Segurança da U/E/O. Esta lista deverá incluir nome, posto e credenciação de cada indivíduo e pode ainda contemplar elementos de empresas que prestem apoio à manutenção do sistema.

A.3.6 Acesso do Pessoal de Manutenção do Sistema

Todo o pessoal militar e civil com responsabilidades de prestar suporte à operação do DCIas, deverá possuir a credenciação de NACIONAL SECRETO. Em caso de necessidade de acesso não prevista por pessoal sem o nível de credenciação necessário, deverão fazer-se acompanhar permanentemente por elementos designados pelo LCISSO. Os acompanhantes deverão ter o grau de credenciação mais elevado, estarem cientes das implicações de segurança das atividades a realizar no âmbito da intervenção e terem controlo permanente sobre as mesmas.

A.3.7 Procedimentos para Pessoal Não Autorizado

Visitantes, funcionários contratados e aqueles que não possuem a autorização de segurança necessária ou necessidade de conhecer, e necessitam de acesso às áreas do DCIas devem ser escoltados para evitar qualquer acesso não autorizado a informação classificada.

Todas as visitas escoltadas às áreas do DCIas devem ser registadas num livro de registos.

A.3.8 Requisitos de treino de segurança

Todos os potenciais utilizadores deverão receber formação sobre requisitos de segurança antes de terem acesso ao DCIas. Isto inclui a leitura e compreensão plena dos SecOPs, sendo responsabilidade de cada utilizador estar familiarizado e compreender o conteúdo dos mesmos.

A.4. Segurança da Informação classificada

A informação pode estar contida em dispositivos digitais de armazenamento e em formato de *hardcopy* (papel).

A informação processada pelo sistema pode ser na marca NACIONAL desde o grau NÃO CLASSIFICADO até ao grau de SECRETO. Todos os utilizadores deverão ter pelo menos a “necessidade de conhecer” alguma da informação processada, armazenada e/ou transmitida.

A.4.1 Segurança dos Documentos

Neste tipo de sistemas, o volume e densidade da informação processada, a sua rápida acessibilidade e a facilidade de cópia de dados, reforça a necessidade da implementação de medidas segurança documental rigorosas.

A.4.2 Tipos de Documentos em Utilização

Entende-se por "documento" todas as formas de armazenamento de informação classificada - documentos em papel, suporte digital e outra tipologia.

A.4.3 Responsabilidades e Procedimentos para Inventário de Documentos

O inventário de todos os documentos classificados em CONFIDENCIAL ou SUPERIOR no DCIas deve ser realizado pelo menos mensalmente. É responsabilidade do LCISSE do DCIas realizar esta inspeção. Se forem observadas discrepâncias, elas devem ser imediatamente reportadas ao CISSE do DCIas. Para os documentos processados no sistema MMHS, considera-se como inventário os registos do próprio sistema.

A.4.4 Procedimentos para Discos Rígidos

Todos os discos rígidos (amovíveis) usados em equipamentos do DCIas, deverão ser devidamente etiquetados com a designação DCIas. Marcas adicionais incluem um rótulo de segurança codificado por cores indicando a classificação de segurança mais alta da informação contida no disco. Uma vez atribuída uma classificação de segurança e a informação classificada NACIONAL resida num disco, este disco manterá a classificação de segurança durante todo o seu ciclo de vida, mesmo que a informação seja posteriormente eliminada. Todos os discos rígidos classificados deverão estar sob o controlo do LSA.

A.4.5 Procedimentos para Controlo Documental

Todos os documentos impressos do DCIas que sejam classificados devem ser tratados de acordo com os procedimentos relativos ao manuseamento de informação classificada conforme normativos em referência (GNS e NATO).

A.4.6 Procedimentos para Marcação de Classificação de Documentos

A responsabilidade de atribuir marcas de segurança em documentos nacionais recai sobre o originador do mesmo. Cada documento ou item deverá ser marcado de acordo com seu próprio conteúdo.

A.4.7 Procedimentos para Desclassificação de Documentos

Se for necessário desclassificar um documento, todos os titulares do documento serão informados desta ação. Estes procedimentos são realizados de acordo com as normas de referência (GNS e NATO).

A classificação de segurança só pode ser diminuída com a autorização do proprietário/originador da informação. Se apenas partes de um documento forem usadas num documento diferente, a classificação de segurança do original não poderá ser diminuída.

A.4.8 Acesso ao Sistema

O uso não autorizado, incluindo o acesso não autorizado a computadores, programas e dados e/ou a sua modificação, constitui uma infração de segurança que poderá resultar em processos criminais, disciplinares ou administrativos.

Os utilizadores não devem ignorar as medidas de segurança implementadas, modificar quaisquer programas ou aceder a qualquer área para a qual não estejam devidamente autorizados.

A.4.9 Impressões em papel

Só as impressoras que integram o DCIas estão autorizadas a imprimir/digitalizar/copiar documentos do DCIas.

A impressão de informação com o grau SECRETO deve ser evitada. Caso exista necessidade da sua impressão, devem ser seguidos procedimentos de controlo para informação com o grau SECRETO.

Por norma, as impressoras do DCIas devem estar colocadas nos Posto de Controlo de Informação Classificada, que deverá também possuir o sistema SEIF. Qualquer utilizador pode imprimir, mas só recebe a impressão depois de o operador do SEIF, ou o chefe do Posto de Controlo, validar a classificação do documento.

É responsabilidade do utilizador garantir que todos os documentos impressos possuem a classificação adequada. Em caso de dúvida relativamente à classificação correta, a impressão deve ser marcada e tratada como NACIONAL SECRETO até que a classificação correta possa ser determinada.

Todos os utilizadores devem garantir que nenhuma impressão é esquecida na impressora. Deve ser dada especial atenção ao número expectável de páginas a imprimir e de que todas são recuperadas.

Todos os documentos impressos devem ser registados no formulário de "Controlo das Impressões em Papel" de acordo com o anexo I, por cada utilizador em cada local da impressora.

Adicionalmente, a impressão de qualquer documento NACIONAL CONFIDENCIAL ou SECRETO deve ser registada no SEIF.

Caso ocorra alguma anomalia no funcionamento da impressora durante a operação de impressão ou cópia, o utilizador deve garantir que todos as folhas no interior da máquina (bandejas de papel excluídas) sejam removidas para evitar o comprometimento potencial da informação classificada. Qualquer defeito que não possa ser corrigido pelo utilizador deve ser reportado imediatamente ao LSA do DCIas.

A destruição de documentos SECRETO deve ser feita de acordo com as instruções de segurança em vigor.

A.4.10 Procedimentos de Transferência de Informação

Os procedimentos de transferência de informação incluem a extração de dados do DCIas e a inserção de dados no DCIas.

A extração de dados em formato digital só é possível através de um pedido de gravação de dados, anexo H, criado pelo utilizador com justificação e autorização.

O LCISSE aprova todos os pedidos de gravação de dados. Uma vez concedida a aprovação, os dados são gravados e marcados pelo LSA e disponibilizados para o utilizador.

O LSA aprova todos os pedidos de entrada de dados. Uma vez concedida a aprovação, o acesso é disponibilizado ao utilizador.

A.5. Segurança do SIC

Cada utilizador é individualmente responsável pelo cumprimento das medidas de segurança descritas nos SecOPs. Os utilizadores devem ter sempre presente que todas as atividades realizadas na utilização do sistema estão sujeitas a monitorização e que podem ser responsabilizados pelas mesmas.

A.5.1 Configuração do Computador

Todos os equipamentos do DCIas devem ser inspecionados, testados pelo SA e validados pelo Cisse antes de serem colocados em produção em qualquer nó/extensão.

A configuração local de *hardware* e *software* do sistema não deverá ser alterada sem autorização prévia. Se o utilizador necessitar de alguma alteração, os procedimentos de configuração deverão respeitar o preconizado no anexo G.

Apenas os componentes de *hardware* e *software* registados oficialmente e validados estão autorizados no DCIas. Quaisquer outros equipamentos ou dispositivos estão proibidos, nomeadamente dispositivos de armazenamento amovível, computadores portáteis, periféricos, etc.

Todos os procedimentos para início e fecho de sessão, ligar e desligar máquina, e outras situações relativas à segurança devem estar descritos em documentação específica (listas de verificação) a elaborar pelo LSA em cada local.

A.5.2 Proteção contra *Software* Malicioso

O *software* antivírus dedicado é instalado em todas as estações de trabalho e alguns servidores e ativado no modo de atualização automática.

Apesar da implementação de medidas automatizadas, os utilizadores devem evitar a introdução de *software*. Mesmo uma rede bem projetada e gerida pode ser comprometida como resultado de novas ameaças, como seja *malware*, ou comportamento negligente dos utilizadores. Assim, os utilizadores devem adotar as seguintes medidas preventivas:

- Verificar regularmente se o *software* antivírus da estação de trabalho está atualizado e, caso contrário, entrar em contato com o LSA/*Service Desk*;
- Não usar dispositivos de armazenamento amovível;
- Se for observado um comportamento suspeito do sistema, parar imediatamente qualquer ação adicional;
- Desligar da rede o equipamento (potencialmente) infetado;
- Notificar imediatamente o *Service Desk*/LSA/LCISSE.

A.5.3 Relatórios de Incidentes de Segurança

Os incidentes de segurança do SIC, deverão ser reportados imediatamente ao *Service Desk* e ao LSA do DCIas. Em alternativa, os incidentes de segurança podem ser reportados diretamente ao SA ou ao CISSE do DCIas.

A notificação inicial de um incidente pode ser realizada por qualquer meio (i.e., telefone, e-mail).

Após o relatório inicial e a avaliação do LSA, o utilizador deverá concluir o relatório de acordo com o anexo F.

Os incidentes de segurança a serem relatados são os seguintes:

- Ataques com códigos maliciosos por programas como vírus, *trojans*, *bugs* e *scripts* não autorizados;

- Acessos ou intrusões não autorizadas ao sistema;
- Utilização de serviços ou equipamentos do sistema não autorizados;
- Uso indevido do sistema, inclusive diferente do propósito oficial;
- Divulgação não autorizada de informação classificada;
- Recolha de informação classificada não autorizada;
- Identificação de vulnerabilidades no sistema;
- Incidentes envolvendo acesso privilegiado ao Sistema;
- Incidentes envolvendo elementos criptográficos e outros elementos COMSEC;
- Incidentes envolvendo o SIC e todos os equipamentos de suporte;
- Incidentes que causam impacto significativo na organização militar;
- Violação de normas de segurança que resultem no comprometimento de informação classificada ou sensível;
- Negação e interrupção dos serviços;
- Espionagem real ou suspeita;
- Outra tipologia de sabotagem real ou suspeita ou catástrofes naturais, acidentais ou negligentes que afetem o sistema e as máquinas em produção.

A.6. Segurança da Emissão

Para garantir a integridade das medidas de Segurança da Emissão (EMSEC), os utilizadores devem assegurar que alterações à cablagem e *hardware* é realizada apenas por pessoal autorizado. Qualquer alteração ao *layout* do equipamento é expressamente proibida sem autorização prévia do CISSO.

A.7. Violações de Segurança

Os utilizadores deverão adotar precauções relativamente a:

- Uso indevido do computador, que inclui, mas não se limita à violação da privacidade de outro utilizador, destruição deliberada de informação ou equipamentos, exploração de vulnerabilidades do sistema, uso de instalações para fins privados ou para processamento de material que traz descrédito à organização militar. (i.e., pornografia, racismo, outro material ofensivo);

- Infrações de segurança, que incluem a divulgação de *passwords* e credenciais de acesso, recursos de segurança do sistema, acesso não autorizado ao sistema e ausência da necessidade de conhecer.

Qualquer violação de segurança relativa ao DCIas, incluindo pessoal, *hardware*, *software*, comunicações, documentos ou segurança física, deve ser imediatamente comunicada ao LSA do DCIas ou ao *Service Desk* do DCIas usando o formulário de relatório de incidente fornecido no anexo F. Dependendo das circunstâncias associadas à violação de segurança, o oficial de segurança da U/E/O, em coordenação com CISSO do DCIas nomeará uma equipa de investigação que determinará:

- Se a informação classificada foi comprometida;
- Em caso afirmativo, se as pessoas não autorizadas que têm ou poderiam ter tido acesso à informação possuem credenciação de segurança e se resultarão danos do comprometimento;
- Recomendação de ação corretiva ou disciplinar (incluindo legal).

A.8. Plano de Contingência do Utilizador

Os utilizadores devem usar o armazenamento disponibilizado em rede (portal *sharepoint*).

Em caso de falha ou mau funcionamento do equipamento, o utilizador deverá efetuar *log off* (se possível) e relatar a falha ao *Service Desk*/LSA.

A.8.1 Plano Contra Incêndios

Os utilizadores do DCIas devem cumprir os procedimentos dos planos contra incêndios e evacuação aplicáveis em cada local.

Em caso de evacuação de emergência, as estações de trabalho e servidores devem ser protegidas por bloqueio ou encerramento, sempre que tal ação não represente um risco pessoal.

A.8.2 Falha de energia/Equipamento

O CISP do DCIas, deve garantir que a energia adequada é fornecida a todos os componentes críticos (rede). O uso de energia da rede, de curto prazo e sem interrupções (UPS) deve ser dimensionado e implementado para fornecer energia elétrica a componentes críticos com base nos seus requisitos de disponibilidade.

A comutação entre fontes de alimentação deve ser testada em intervalos regulares e ao seu desempenho e resultados registados de acordo com as instruções de segurança.

A.8.3 Manuseio de Material Cripto em situações de Emergência

Os administradores e utilizadores do DCIas, devem tomar todas as medidas necessárias para evitar que o material cripto seja acessível a pessoas não autorizadas cumprindo os Planos/Procedimentos de evacuação e destruição de material cripto aplicáveis em todos os locais.

Anexo B – SecOPs para Administradores

Procedimentos Operacionais de Segurança (SecOPs) para Administradores do DCIas

B.1. Introdução

Este anexo constitui os SecOPs do DCIas para ADMINISTRADORES, rede esta que permite armazenar, processar e transmitir informação classificada NACIONAL até e incluindo NACIONAL SECRETO.

Estes SecOPs são emitidos pela Autoridade de Planeamento e Implementação do SIC (CISPIA) de acordo com os requisitos contidos na legislação nacional e também em consonância com política de segurança da NATO [C-M(2002)49] e documentação associada.

Os pontos de contacto listados no anexo J, podem fornecer orientações em caso de dúvidas ou incidentes relacionados com segurança. A atualização da lista de pontos de contacto deve ser feita sempre que aconteçam mudanças dos responsáveis na administração e segurança do sistema.

B.2. Administração e Organização de Segurança

B.2.1 Modo de Operação de Segurança

O Modo de Operação de Segurança para o DCIas é alto nível do sistema, de acordo com o [AC/35-D/2004]. Neste modo de operação, nem todos os utilizadores com acesso ao SIC possuem uma necessidade de conhecer comum, mas todos estão credenciados para o mais elevado grau de classificação de segurança da informação armazenada, processada ou transmitida pelo SIC.

B.2.2 Pedido de acesso ao DCIas

O acesso ao DCIas só pode ser garantido a administradores que tenham completado o procedimento de registo. Todos os administradores do DCIas com privilégios de administração total, deverão ter a sua credenciação válida em NACIONAL MUITO SECRETO. No caso dos administradores com privilégios locais, deverão ter credenciação válida para NACIONAL SECRETO.

Quando um utilizador submete um formulário “Pedido de Acesso” preenchido (Anexo C), o SA/Service Desk irá criar as necessárias credenciais de Utilizador seguindo as definições e

requisitos SIC para o DCIas e de acordo com os normativos em vigor. Na ativação das credenciais de acesso, o utilizador recebe uma *password* ‘one-time use only’, sendo obrigado a efetuar a sua alteração no primeiro “log in”.

A duração do acesso é limitada ao período de validade da credenciação do utilizador e/ou saída do local/pedido de acesso ao DCIas. O CISSO e o SA estão autorizados em qualquer momento e sem aviso prévio suspender o acesso ao sistema, através da desativação da conta, até à resolução do problema de segurança que originou a suspensão.

Não é permitida a partilha de credenciais no DCIas.

A atribuição de privilégios diferenciados a utilizadores tem de ser aprovada pelo CISSO e implementada pelo SA. O SA/Service Desk deverá manter uma listagem de utilizadores autorizados.

A utilização de *passwords* previamente utilizadas é negada.

As credenciais serão automaticamente bloqueadas após três (3) tentativas de acesso falhadas. Igualmente serão manualmente bloqueadas se se suspeitar que as credenciais estão a ser alvo de utilização incorreta, ou não utilizada (*logged in*) por mais de 180 dias.

O desbloqueio de credenciais de utilizador requer a intervenção do SA/Service Desk. O desbloqueio de credenciais com privilégios escalados (i.e., *root*, *sysadmin*) requer autorização prévia da CISOA.

As credenciais não necessárias deverão ser bloqueadas ou eliminadas.

B.2.3 Desativar credenciais do DCIas

Após a saída do utilizador, ou revogação da sua credenciação, as suas credenciais devem ser imediatamente desativadas ou transferida para o sucessor. Credenciais para efeitos de treino devem ser desativadas após o término da ação de formação.

As credenciais bloqueadas por 180 dias sem qualquer solicitação de ativação devem ser eliminadas permanentemente.

B.2.4 Identificação e Autenticação

O acesso ao DCIas é concedido apenas a indivíduos que concordam em assumir a responsabilidade pessoal pela proteção de informação classificada até ao grau SECRETO. A partilha de credenciais não está autorizada no DCIas.

A identificação e autenticação do utilizador no DCIas, consiste em cada utilizador inserir o seu ID, a respetiva *password* associada e escolher de uma lista de funções autorizadas antes de receber acesso ao sistema. As medidas de controlo de identificação e autenticação para ao DCIas são:

- Identificação do utilizador - Para cada utilizador é fornecido um *User ID* que identifica exclusivamente o utilizador do DCIas, pela sua função dentro da organização;
- Autenticação - Uma *password* é usada para autenticar exclusivamente cada utilizador no DCIas. A partilha de credenciais entre utilizadores é proibida;
- Quando autenticado no sistema, o ID do utilizador é usado para auditar e rastrear o uso do DCIas;
- A *password* dos utilizadores é classificada como SECRETA após um utilizador ter feito login com sucesso no DCIas (via ID do utilizador, *password*).

Os requisitos dos mecanismos de controlo de acesso são os seguintes:

- O controlo de acesso discricionário define e controla o acesso entre utilizadores selecionados e objetos selecionados (por exemplo, ficheiros e programas);
- O mecanismo de imposição (por exemplo, controlos próprios/grupo/públicos, listas de controlo de acesso) permite que os utilizadores especifiquem e controlem a partilha desses objetos por indivíduos nomeados ou grupos de indivíduos definidos, ou por ambos;
- O mecanismo de controlo de acesso discricionário, quer seja por ação explícita do utilizador ou por padrão, garante que os objetos são protegidos contra acesso não autorizado;
- A permissão de acesso a um objeto a determinados grupos de utilizadores que ainda não possuem permissão de acesso é atribuída apenas pelo proprietário dos dados.

Eventuais envelopes que contenham *passwords* de credenciais de sistema privilegiadas (por exemplo, Administrador de Sistema) devem ser armazenados com grau SECRETO, para Administradores de Sistema normais, e o grau MUITO SECRETO para Administradores de Sistema com privilégios mais elevados num invólucro com acesso controlado e registado.

B.2.5 Não-Repúdio, Responsabilização e Auditoria

Para garantir que os utilizadores do DCIas estão cientes do nível de responsabilidade, os Administradores do DCIas devem implementar e manter mecanismos de controlo e

procedimentos necessários para a gestão de *logs* de segurança, *logs* de auditoria e os serviços de sistemas de apoio e recursos do DCIas.

Para todos os componentes do sistemas e utilizadores do DCIas, os *logs* de auditoria de segurança e/ou sistema, juntamente com mecanismos e medidas de controlo, devem garantir a recolha, registo, revisão, correlação e armazenamento de informação para eventos específicos relacionados com segurança. Os dados de auditoria devem ser retidos por um período mínimo de cinco (5) anos.

No mínimo, os seguintes eventos auditáveis devem ser recolhidos e registados:

- *Logs* de segurança e auditoria dos servidores do DCIas;
- Informação recolhida de sistemas de Detecção e Prevenção de Intrusão;
- Dados de *syslog* dos principais equipamentos da rede;
- Registos de impressoras e equipamentos de armazenamento amovível.

Estas medidas de auditoria e segurança são necessárias para fornecer informação suficiente para investigar um comprometimento deliberado ou accidental de credenciais, do sistema ou informações de utilizadores do DCIas. O SA e o CISSOA do DCIas devem realizar verificações e avaliações periódicas sobre a implementação completa de todas as medidas de segurança, auditoria e controlo, em vigor. Esta avaliação deve ser realizada pelo menos anualmente.

B.3. Segurança Física

B.3.1 Inspeção de Segurança Física

Cada Oficial de Segurança da U/E/O, é responsável pela inspeção das medidas de segurança em vigor, para proteger os locais físicos onde o DCIas possui meios instalados. Uma verificação inicial completa e exaustiva, deverá ser seguida por um ciclo de inspeções periódicas para garantir a segurança da localização física de todos os ativos dos *sites* do DCIas e realizada pelo menos a cada 12 meses. O objetivo desta inspeção é garantir que:

- Todas as estações de trabalho estão localizadas em Áreas de Segurança Classe 1 ou Classe 2;
- Todas as estações de trabalho possuem informações precisas de registo e rotulagem;

- Os registos de eventuais não conformidades devem ser guardados pelo Oficial de Segurança e devem estar disponíveis para consulta durante as inspeções de segurança.

Algumas medidas de proteção física devem ser submetidas a verificações mais frequentes, por exemplo, o perímetro deve ser verificado uma vez por dia e uma vez por noite, rondas aleatórias nas áreas de trabalho (Áreas de Segurança Classe 1 e Classe 2) durante as horas de atividade reduzida.

B.3.2 Conceção de Ambientes de Segurança

Para efeitos das medidas de segurança física do DCIas são distinguidos dois tipos de ambientes de segurança:

- Ambiente de segurança global – área de grandes dimensões (por exemplo, o próprio aquartelamento ou edifício).
- Ambiente de segurança local – área de pequenas dimensões (sala, gabinete) onde os sistemas SIC estão instalados. Este corresponde normalmente a Áreas de Segurança Classe 2 e Classe 1.

B.3.3 Controlo de Acessos a Pessoal e Equipamento

O pessoal e os equipamentos eletrónicos pessoais e de serviço, que acedam ao ambiente de segurança local estão sujeitos a verificação de segurança prévia e requerem validação por um elemento da estrutura de segurança: Oficial de Segurança da U/E/O, LCISSE ou CISSE.

Se for necessário o acesso a equipamento COMSEC, os Procedimentos de Controlo COMSEC (Ref. [SDIP-293]) devem ser aplicados.

B.4. Segurança do Pessoal

B.4.1 Requisitos de Credenciação

Os indivíduos autorizados a ter acesso ao DCIas, deverão possuir credenciação no mínimo, NACIONAL SECRETO, válida pela duração do período de acesso. A credenciação é específica para cada utilizador com necessidade de conhecer relativa a alguma da informação processada, armazenada e/ou transmitida no DCIas.

O acesso ao equipamento COMSEC do DCIas é limitado ao pessoal que possui autorização COMSEC apropriada e faz parte da Cadeia de Custódios Cripto do Exército.

Todos os Administradores de Sistema do DCIas (SA) com privilégios de administração devem ter um certificado MUITO SECRETO válido.

Os Administradores de sistema com privilégios locais limitados (LSA) devem ter um certificado válido de pelo menos NACIONAL SECRETO.

Durante exercícios envolvendo o DCIas, somente pessoal autorizado deverá ter acesso às áreas onde a rede está instalada.

B.4.2 Equipa de Custódios Cripto

A equipa de custódios Cripto para o DCIas, incluindo o Custódio Cripto e o Custódio Cripto Substituto, é a equipa do restante material cripto da U/E/O e deve ser credenciada para o nível do material criptográfico mantido na sua conta COMSEC.

B.4.3 Passwords

A *password* de credenciais com privilégios escalados (i.e., *root*, *sysadmin*) deverá ter pelo menos 12 caracteres.

As regras de composição da *password* de credenciais com privilégios escalados exigem a inclusão de 4 dos 4 conjuntos de caracteres seguintes: letras minúsculas (a..z), letras maiúsculas (A..Z), números (0..9) e caracteres especiais (~ ! @ # \$ % ^ & * () _ + | ` - = \ { } [] : " ; ' < > ? , . /).

Credenciais com privilégios escalados (i.e., *root*, *sysadmin*) devem ser alteradas sempre que houver suspeita de comprometimento ou divulgação a uma pessoa não autorizada e pelo menos uma vez a cada 90 dias.

Os envelopes que contém *passwords* de credenciais com privilégios escalados devem ser armazenados, pelo menos, como informação SECRETA num contentor de segurança aprovado com acesso controlado e registado.

B.5. Segurança da Informação Classificada

B.5.1 Procedimentos para encerramento, destruição ou alienação do sistema

O SA deve manter uma estreita ligação com o CISSO, que é normalmente o responsável pelas seguintes atividades relacionadas com o cancelamento do serviço e a descontinuação de equipamentos usados no DCIas:

- Realizar o arquivamento, desclassificação e/ou destruição apropriada dos meios de armazenamento associados a o DCIas, garantindo os registos necessários;
- Realizar o arquivamento ou destruição apropriada da documentação impressa associada.

Como princípio orientador, os dispositivos de armazenamento usados no DCIas não são desclassificados, mas mantidos para reutilização no nível SECRETO, se aplicável.

Procedimentos apropriados para alienação e destruição de material criptográfico do DCIas e sistemas criptográficos e os seus materiais associados devem seguir os procedimentos e processos do [SDIP-293].

B.6. Segurança SIC

Diferentes tipos e camadas de mecanismos de segurança são aplicados no DCIas para construir o nível de segurança necessário. Estes mecanismos de segurança podem contribuir separadamente ou em combinação com outros para alcançar os objetivos de segurança da Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-repúdio e, portanto, fornecer um nível aceitável de segurança com a gestão dos riscos de segurança residuais para fornecer uma postura de segurança forte o suficiente para a operação do DCIas.

B.6.1 Segurança de *Hardware*

Todos os equipamentos do DCIas devem ser protegidos de fatores ambientais que possam causar danos no sistema. Estes incluem poeira, humidade alta, calor e aerossóis que podem penetrar pelas aberturas de ventilação e danificar o equipamento.

O equipamento do DCIas deve ser colocado fisicamente de acordo com requisitos TEMPEST e os critérios de instalação pertinentes para equipamentos elétricos e eletrónicos (Ref. [SDIP-29]) para atender aos critérios de *zoning* (Ref. [SDIP-28]).

Qualquer equipamento que processe ou exiba informações do DCIas (estações de trabalho, monitores, impressoras, etc.) deve ser certificado para processar informação até e inclusive SECRETO.

A colocação física do(s) monitor(es) deve evitar a visualização do conteúdo do ecrã por pessoas não autorizadas.

B.6.2 Impressoras

Todas as impressoras ligadas ao DCIas devem estar conectadas à rede, permitindo assim que o LCISSO audite e rastreie os documentos impressos. Os dispositivos da impressora não devem ser compartilhados com redes de diferentes classificações por meio de caixas de comutação manuais ou automatizadas.

Apenas as impressoras controladas localizadas nas áreas do DCIas estão autorizadas a imprimir/digitalizar/copiar documentos no DCIas.

As impressoras com capacidade de armazenamento (discos rígidos ou outras formas de armazenamento persistentes) só podem ser localizadas em áreas controladas (como Áreas de Segurança Classe 1). No caso destas impressoras, os respetivos discos passam a ser classificados como SECRETO devendo cumprir com as regras de segurança para este tipo de informação. Deste modo, todas as impressoras deverão ser propriedade do Exército não podendo ser alugadas.

B.6.3 Marcação e Controlo da Saída da Impressora

É responsabilidade do utilizador garantir que todos os documentos impressos tenham a classificação adequada. Em caso de dúvida relativamente à classificação correta, a impressão deve ser marcada e tratada como NACIONAL SECRETO até que a classificação correta possa ser determinada.

Todos os utilizadores devem garantir que nenhuma impressão é esquecida na impressora. Deve ser dada especial atenção ao número expectável de páginas a imprimir e de que todas são recuperadas.

Todos os documentos impressos devem ser registados no formulário de "Controlo das Impressões em Papel" de acordo com o anexo I, por cada utilizador em cada local da impressora.

Adicionalmente, a impressão de qualquer documento NACIONAL SECRETO deve ser registada por cada utilizador.

Caso ocorra alguma anomalia no funcionamento da impressora durante a operação de impressão ou cópia, o utilizador deve garantir que todos as folhas no interior da máquina (bandejas de papel excluídas) sejam removidas para evitar o comprometimento potencial da informação classificada. Qualquer defeito que não possa ser corrigido pelo utilizador deve ser reportado imediatamente ao LSA do DCIas.

A destruição de documentos SEGRETO deve ser feita de acordo com as instruções de segurança em vigor.

B.6.4 Segurança do *Software*

O sistema operativo e outro *software* de segurança devem ser implementados e verificados quanto à conformidade com as configurações aprovadas para conformidade de segurança. Os *patches* de segurança para vulnerabilidades no sistema operativo e no *software* aplicativo, informados pelos boletins de segurança dos fabricantes, devem ser aplicados de maneira expedita, a menos que razões operacionais justifiquem o contrário. Recomendações sobre vulnerabilidades e a aplicabilidade de *patches* devem ser solicitadas ao CISSO.

A instalação do *software* no DCIas é apenas autorizada aos administradores do sistema (SA) do DCIas. Esta aprovação requer uma validação prévia do CISSO, em conformidade com a Lista de Produtos aprovada.

B.6.5 Vírus / Prevenção de *Software* Malicioso

Os administradores do sistema do DCIas (SA e LSA) são responsáveis por garantir que a proteção antivírus é executada nos servidores e estações de trabalho dos utilizadores e é atualizada em relação aos mecanismos de pesquisa e arquivos de definição.

Os procedimentos incluem o seguinte:

- Verificação do *software* do sistema operativo instalado, pacotes de *software* e programas utilitários quanto à presença de *software* malicioso incluindo os procedimentos para apagar *software* malicioso detetado;
- Verificação de meios de armazenamento removível recebidos de fontes externas;
- Verificação de ficheiros recebidos de fontes externas quanto à presença de *software* malicioso;
- Aconselhar os utilizadores sobre a deteção de eventos de *software* malicioso;
- Informar imediatamente o SA/Service Desk e o CISSO se um *software* malicioso for detetado.

Os mecanismos de *software* malicioso do DCIas incluem:

- Servidor de gestão de segurança central de antivírus;
- *Software* antivírus para servidores e estações de trabalho.

B.6.6 Backups do Sistema

Os Administradores do Sistema do DCIas devem garantir que são realizados, com regularidade, *backups* de todas as informações do sistema e do utilizador mantidas nos servidores. Os *backups* devem ser devidamente protegidos de acordo com sua classificação e preferencialmente armazenados num cofre à prova de fogo em local externo.

Como o utilizador deve estar ciente de que não é permitido armazenar informação (ficheiros, e-mails ou informação semelhante) na(s) unidade(s) de disco rígido local, todas as informações dos utilizadores contidas nas unidades de rede serão copiadas.

B.6.7 Manutenção e Disponibilidade dos Dados de Auditoria

Os registos de segurança e auditoria ao DCIas devem ser gerados para cada um dos seguintes eventos auditáveis, devendo estar associadas identidades de utilizadores individuais a esses eventos, bem como devem incluir data e hora do evento:

- *Start-up*, *re-starts* e *shutdown* do Sistema;
- Tentativas de *log on* e *log off* de utilizadores individuais;
- Alterações nas permissões e privilégios de utilizadores e grupos;
- Alterações nas informações de gestão do sistema relevantes para a segurança, incluindo as funções de auditoria;
- *Start-up* e *shutdown* da função de auditoria;
- Qualquer acesso a dados de segurança;
- Eliminação, criação ou alteração de registos de auditoria de segurança (*security audit records*);
- Alterações na data e hora do sistema;
- Tentativas falhadas de acesso aos recursos do sistema.

O SA do DCIas é responsável pela manutenção e disponibilidade dos registos de segurança e auditoria. A gravação, *backup* e manutenção desses registos é obrigatória e deve incluir todos os tipos de eventos (eventos bem-sucedidos e malsucedidos). A retenção de arquivos de auditoria é abordada em [AC/35-D/2004].

B.7. Gestão da Segurança e Auditoria

A análise periódica deve ser realizada na informação de registo (*accounting information*) para detetar ações tentadas ou concluídas que possam violar a segurança.

Toda a violação dos regulamentos de segurança, violação dos controlos de segurança e falha no cumprimento dos procedimentos de segurança impostos por estes SecOPs, quer sejam identificados por meio da análise da informação de registo (*accounting information*) ou por outros meios, devem ser relatados imediatamente ao LCISSO e/ou CISSO.

O SA notificará o CISSO no caso de um mau funcionamento da auditoria. O CISSO deve investigar e relatar suas descobertas à CISOA.

B.8. Segurança Criptográfica

O Oficial COMSEC do DCIas é responsável pela implementação e procedimentos de controlo de segurança criptográfica e pela credenciação do pessoal e requisitos de “doutrina criptográfica”.

Os procedimentos criptográficos específicos para o DCIas são:

- Apenas o pessoal especificamente designado por escrito, e constante da Cadeia de Custódios Cripto do Exército, poderá ter acesso autorizado ao material criptográfico;
- As operações e procedimentos básicos para a utilização de equipamento criptográfico estão detalhados nos respetivos manuais do operador;
- O pessoal com acesso atribuído e responsável pelo equipamento/material criptográfico deve estar familiarizado com os procedimentos locais de manuseio criptográfico. Além disso, o pessoal deve ser proficiente na operação de equipamentos criptográficos sob a sua responsabilidade.

Se o equipamento/material criptográfico estiver fisicamente colocado na mesma área de acesso controlado com outros equipamentos de rede, todos os utilizadores (incluindo os administradores do sistema) com acesso físico ao equipamento/material criptográfico devem ser informados sobre os procedimentos de segurança criptográfica.

B.9. Segurança da Emissão

O CISSO e a SAA do DCIas são responsáveis pela implementação e procedimentos de controlo dos requisitos de Segurança da Emissão (EMSEC).

Todos os equipamentos e instalações do DCIas devem ser implementados e operados de acordo com os requisitos de segurança SIC da NATO em EMSEC (Ref. [AC/322-D(2007)0036], [SDIP-28], [SDIP- 29] e Diretiva da NCIA N.º 90-5).

B.10. Plano de Emergência

B.10.1 Plano de Contingência

Estes procedimentos de contingência para o DCIas devem ser usados em todas as instalações existentes e incluem a manutenção de *backups* de dados e programas essenciais do sistema e identificação de meios alternativos para manter a continuidade operacional do sistema. Procedimentos contemplados nos planos de contingência, incluindo *backups* e procedimentos de recuperação, devem ser exercitados pelo menos anualmente, devendo ser feito registo dessas evidências que possam vir a ser fornecidas aquando de inspeções.

B.10.2 Planos de Continuidade Operacional e *Backups*

Planos de recuperação detalhados devem ser formulados e testados para garantir que em caso de falha do DCIas, a continuidade operacional pode ser restabelecida no mínimo período de tempo.

O plano de recuperação (*Disaster and Recovery Plan* - DRP) deve ser ativado pelo SA, sempre que um cenário causar a interrupção da operação do nó/extensão do DCIas.

O CISP do DCIas deve definir a frequência do processo e procedimentos de *backup*, em conjunto e de acordo com os requisitos e necessidades do utilizador do DCIas para o *backup* de sistemas e dados.

Os Administradores do DCIas devem seguir os procedimentos de *backup* estabelecidos pela CISPIA e/ou CISOA do DCIas. A implementação desses procedimentos de *backup* é vital para os planos de emergência e contingência. O objetivo é evitar a perda de informação/dados e disponibilidade do próprio DCIas. Os detalhes dos métodos operacionais para *backups* de informações relevantes para a segurança e do utilizador devem estar disponíveis para utilizadores e administradores dos sistemas.

Os suportes físicos de *backup* deverão ser classificados e rotulados como SECRETO e armazenados de acordo com essa classificação à responsabilidade do SA.

Os *backups* mensais deverão ser mantidos por um período mínimo de 12 meses. Os *backups* semanais devem ter um ciclo de 5 semanas e os *backups* diários um ciclo de 8 dias, sendo os dados substituídos automaticamente.

O acesso às cópias de *backup* é limitado ao SA e ao CISSO ou a quem estes delegarem.

B.10.3 Gestão de Configurações

A gestão de configurações do DCIas está sob a direção do CISP e pode ser delegada no SA do DCIas.

A gestão de configurações consiste nas medidas e requisitos de segurança para identificar, controlar, contabilizar, divulgar e auditar todas as alterações feitas durante as fases de projeto, desenvolvimento, operação, manutenção e atualizações durante o ciclo de vida do DCIas.

Todas as alterações, modificações ou atualizações dos componentes de *hardware* ou *software* do DCIas estão sujeitas à gestão de configurações. Aqueles que afetam as operações seguras do sistema devem ser revistos pelo CISSO e aprovados pela CISOA antes da sua implementação.

O SA é a única entidade responsável pelo desenvolvimento de processos e procedimentos detalhados de gestão de configuração.

Todas as alterações de configuração devem seguir os procedimentos de gestão de configuração constantes no Anexo G.

O LSA/SA deve cumprir os requisitos de segurança para a gestão de configuração e apoiar o papel do LCISSO/CISSO para garantir a disponibilidade e integridade, mas também a confidencialidade, autenticidade e não-repúdio, no DCIas e seus componentes individuais, por meio de verificações periódicas e sensibilização para a cultura de segurança.

Os Administradores do DCIas são responsáveis por acompanhar a implementação das atualizações de configuração e a documentação que descreve a *baseline* da configuração autorizada do DCIas que eles utilizam.

Para garantir que nenhuma alteração não autorizada nesta *baseline* é realizada, os direitos de administração são atribuídos apenas ao SA do DCIas e quaisquer alterações devem ser validadas pelo CISSO.

O DCIas segue a doutrina e diretivas do GNS, que estão em linha com as da NATO, nomeadamente em todos os assuntos relacionados com alterações de configuração, em

particular atualizações do *software* do sistema operativo, incluindo utilitários e pacotes de *software* e antivírus que foram previamente testados e autorizados.

Anexo C – Formulário de Pedido de Acesso

CRIAÇÃO/ALTERAÇÃO/ELIMINAÇÃO DE CONTA DO DCLAS		
IDENTIFICAÇÃO DO REQUERENTE	U/E/O:	
	POSTO/NIM/NOME:	
	FUNÇÃO:	CONTATO:
	DATA / ASSINATURA:	
CREDENCIAÇÃO	GRAU:	
	VALIDADE:	
	Nº DO CERTIFICADO DE SEGURANÇA:	
MOTIVO PEDIDO DE CONTA: Selecionar opção adequada e justificar	NOVA CONTA <input type="checkbox"/>	
	ALTERAÇÃO DADOS <input type="checkbox"/>	
	RENDIÇÃO <input type="checkbox"/>	
NOME DO TERMINAL ONDE IRÁ ACEDER (a preencher pelo Administrador de Rede Local - LSA)		
AUTORIZAÇÃO DATA – POSTO/NIM/NOME - ASSINATURA		
OFICIAL DE SEGURANÇA LOCAL DO SIC (LCISSO)		
OFICIAL DE SEGURANÇA DO SIC (CISSO)		
Implementação pelo Administrador do Sistema (SA) / Service Desk		
username@rsexercito.local		
OBSERVAÇÕES		
DATA - POSTO/NOME - ASSINATURA		

(Formulário a ser enviado pelas U/E/O ao CGIC [cgic@exercito.pt])

Página intencionalmente em branco

Anexo D –*Brí핑ue* de Segurança

BRÍFINGUE DE SEGURANÇA DO DCLAS

Objetivo: Definir e clarificar as responsabilidades individuais da utilização da *password* no acesso aos sistemas de informação classificados.

Geral: A segurança do DClas é baseada no princípio da necessidade de conhecer, sendo da responsabilidade individual de cada utilizador o controlo da respetiva conta atribuída. Os controlos técnicos e procedimentais integrados no sistema são necessários para garantir a proteção adequada ao sistema e aos dados aí armazenados.

Responsabilidades individuais: O ónus da responsabilidade pela segurança da informação classificada armazenadas no sistema, em última análise, recai sobre cada indivíduo que tem acesso ao sistema. Independentemente das medidas de segurança e de salvaguarda implementadas, esses controlos não serão suficientes se cada pessoa que usa o sistema não cumprir as suas responsabilidades pela segurança da informação. Lembre-se de que as suas credenciais de utilizador serão ativadas somente depois de ler os Procedimentos de Operação de segurança (SecOPs) do DClas. Deverá ser conhecedor de quem é o administrador de rede local (LSA) e o oficial de segurança local (LCISSO).

A. As principais responsabilidades de cada utilizador do DClas são:

1. Não está autorizado o uso do computador da rede classificada (DClas) em redes não classificadas. É estritamente proibido e pode resultar em ações disciplinares contra o utilizador.
2. A *password* de acesso ao sistema é pessoal e intransmissível, não sendo permitido a sua divulgação, independentemente da situação ou circunstâncias. Essa divulgação ou uso é considerada uma violação de segurança e resultará na suspensão do acesso ao sistema.
3. Deverá informar imediatamente qualquer suspeita de comprometimento da sua *password* ao LSA ou LCISSO.
4. As *passwords* devem ter pelo menos 9 caracteres alfanuméricos, com pelo menos uma letra, dois números e um caracter especial, com uma combinação de letras minúsculas, maiúsculas, números e caracteres especiais (por exemplo, ~,!, @, #, \$, ^, |, +, [, etc.).
5. Não deverá usar nomes, palavras, palavras de código, acrónimos comuns ou qualquer referência que possa ser encontrada num dicionário. Lembre-se que cabe ao utilizador proteger os dados armazenados no sistema.
6. É da responsabilidade do utilizador, controlar o acesso e o uso adequado dos ficheiros particulares armazenados, sob a sua identificação de utilizador e a *password*. O utilizador é

responsável pelo uso adequado desses ficheiros, pelas marcações e a correta classificação, assim com pelas modificações feitas no documento.

7. Deverá informar o LSA de qualquer alteração que, na sua opinião, deva ser feita na classificação ou na sua pasta de arquivo.

8. Reportar imediatamente ao LSA, qualquer indicação de possível mau funcionamento do sistema, incluindo bloqueio das credenciais de acesso.

B. Existem várias medidas específicas que devem ser sempre tomadas para proteger o sistema de possíveis comprometimentos, que são:

1. Verificar se nenhuma outra pessoa está em posição de visualizar a digitação da sua *password*.

2. Reportar imediatamente ao LSA ou LCISSO, qualquer resposta do sistema inválida, inconsistente ou inesperada.

3. Certifique-se que, sempre que modificar um documento, a classificação de segurança foi colocada de forma correta.

4. Certifique-se que todos os documentos impressos, discos rígidos, *pen drives*, etc., são manuseados e armazenados de acordo com a classificação atribuída.

5. Faça *log off* corretamente no final de cada sessão. Reporte imediatamente ao LSA se a máquina não efetuar adequadamente este procedimento (*log off/log out*).

Posto/NIM/Nome:

Data:

Assinatura:

Anexo E - Declaração de Conhecimento dos SecOPs

DECLARAÇÃO DE CONHECIMENTO DOS SECOPS DO DCLAS

Li e compreendi os procedimentos de segurança definidos nos SecOPs do DClas.

Comprometo-me a respeitar e esforçar-me-ei no cumprimento dos procedimentos descritos nos SecOPs do DClas.

☒ DClas

U/E/O _____

USER ID:

POSTO/NIM/NOME:

TELF.:

DATA:

ASSINATURA (UTILIZADOR):

CONTA ATIVADA:

ASSINATURA

DO OFICIAL DE SEGURANÇA LOCAL DO SIC (LCISSO):

(Para ser arquivado pelo LCISSO depois de preenchido)

Página intencionalmente em branco

Anexo F – Formulário de Relatório de Incidente de Segurança

RELATÓRIO DE INCIDENTE DE SEGURANÇA NO DCLAS

Número do Relatório de Incidente	
----------------------------------	--

Para ser preenchido para todos os incidentes de segurança identificados no DCLas.

1. Notificação

Relatado por (Posto/NIM/Nome)	U/E/O	Telefone	Data

2. Detalhes do Incidente

Data da ocorrência do Incidente	
Data detecção do Incidente	
Localização Incidente	
Pessoa(s) Envolvida(s)	
Tipo de Incidente	
Ataques de código malicioso por programas tais como vírus, cavalos de Tróia, <i>bugs</i> e <i>scripts</i> não autorizados	<input type="checkbox"/>
Acesso não autorizado ao sistema ou intrusão	<input type="checkbox"/>
Utilização não autorizada a serviços do sistema ou equipamentos	<input type="checkbox"/>
Uso indevido do sistema inclusive para o uso não oficial	<input type="checkbox"/>
Divulgação não autorizada de informação classificada	<input type="checkbox"/>
Recolha não autorizada de dados importantes	<input type="checkbox"/>
Descoberta de quaisquer vulnerabilidades no sistema	<input type="checkbox"/>
Incidentes envolvendo acesso privilegiado ao SIC	<input type="checkbox"/>
Incidentes envolvendo elementos criptográficos e outros elementos COMSEC	<input type="checkbox"/>
Incidentes envolvendo o SIC e todos os equipamentos de apoio	<input type="checkbox"/>
Incidentes com impacto significativo na organização militar	<input type="checkbox"/>
Violação das normas de segurança resultem no comprometimento de informação classificada	<input type="checkbox"/>
Negação e interrupção de serviços	<input type="checkbox"/>
Espionagem real ou suspeita	<input type="checkbox"/>
Sabotagem real ou suspeita, catástrofes naturais, acidentais ou negligentes que afetem o sistema	<input type="checkbox"/>

Fornecer quaisquer comentários adicionais ou detalhes do incidente no máximo possível.

Informação Adicional	N/A	Não	Sim	Detalhes
O dispositivo tinha conectividade de rede?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Estava armazenada no dispositivo alguma informação pessoal, ou organizacional?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Alguma da informação foi do conhecimento da Comunicação Social?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A informação do conhecimento do público estava encriptada e protegida por <i>password</i> ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Esteve envolvido algum dispositivo de armazenamento portátil?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A informação contida no dispositivo de armazenamento portátil estava encriptada e protegida por <i>password</i> ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

3. Equipa SIC

NOME	Data de Receção	Ações desenvolvidas	Assinatura		
Administrador de Rede Local (LSA)					
Oficial de Segurança Local do SIC (LCISSO)					
Relatório de Informações			N/A	Não	Sim
O CTE foi informado?			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
O CGIC foi informado?			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

4. Conclusão

Autoridade	NOME	Ações Finais	Assinatura
CISAO			

Anexo G – Formulário de Pedido de Alteração de Configuração

FORMULÁRIO DE PEDIDO DE ALTERAÇÃO DE CONFIGURAÇÃO DO DCLAS

Número do Pedido:	
-------------------	--

Para ser preenchido para todos os Pedidos de Alteração de Configurações.

1. Identificação

Pedido por Posto/NIM/Nome)	U/E/O	Telefone	Data do Pedido

2. Detalhes do Sistema

Nome do Sistema:	DCLas
Baseline do Sistema:	
Estado da Acreditação do Sistema:	

3. Descrição da Alteração

Fornecer todos os detalhes necessários para a seu pedido de alteração

Tipo de Alteração	Sim	Detalhes
Novo(s) dispositivo(s) na rede (e.g. <i>router, switch, firewall</i> , entrada VPN)	<input type="checkbox"/>	
Novo(s) servidor(es)	<input type="checkbox"/>	
Nova(s) estação(ões) de trabalho (<i>desktops</i> ou <i>laptops</i>)	<input type="checkbox"/>	
Outro <i>hardware</i> novo	<input type="checkbox"/>	
Desativação de <i>hardware</i> existente	<input type="checkbox"/>	
Novo servidor virtual	<input type="checkbox"/>	
Novo Sistema Operativo	<input type="checkbox"/>	
Atualização de Sistema Operativo existente	<input type="checkbox"/>	
Novo pedido aplicação	<input type="checkbox"/>	
Atualização ou melhoria da aplicação	<input type="checkbox"/>	
Nova página <i>Web Site</i> ou <i>Web Link</i>	<input type="checkbox"/>	
Novo <i>link</i> da página <i>Web</i>	<input type="checkbox"/>	
Atualização ou correção de <i>bug</i> em página <i>Web</i> existente	<input type="checkbox"/>	

Novo DBMS (e.g, MS SQL Servidor ou Oracle)	<input type="checkbox"/>	
Adição de nova estação de Base de Dados (DB)	<input type="checkbox"/>	
Alteração de uma estação de DB existente (e.g., alterações a uma tabela)	<input type="checkbox"/>	
Aplicativo ou serviço de <i>middleware</i> novo ou atualização	<input type="checkbox"/>	
Alteração nas portas, protocolos, e serviços usados ou fornecidos pelo sistema	<input type="checkbox"/>	
Alterações destinadas a atender aos requisitos de segurança ou melhorar a segurança do sistema (e.g. módulos criptográficos, <i>patch</i> de segurança, autenticação, autorização, alteração de funções)	<input type="checkbox"/>	
Novo tipo de informação processada, armazenada, ou transmitida no sistema	<input type="checkbox"/>	
Mudança de Interface (adição/remoção)	<input type="checkbox"/>	
Mudança de Localização	<input type="checkbox"/>	
Outra alteração	<input type="checkbox"/>	

4. Justificação da Alteração

Fornecer os detalhes necessários para a justificação do pedido de alteração:

--

Assinale o que será afetado por este pedido de alteração					
Segurança do Pessoal	Segurança Ambiental	Segurança do Equipamento	Capacidade Operacional	Segurança Militar	Outro
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Obsolescência	Confiança	Manutenção	Performance	Requisitos Legais	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Que impactos podem ser antecipados?		N/A	Não	Sim	Comentários
Há impacto de segurança com a alteração?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Há impacto funcional com a alteração?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Há impacto operacional com a alteração?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Qual pode ser o impacto esperado de NÃO FAZER a alteração?		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Este pedido para um problema específico, é:			Prioridade Proposta:		
Permanente	Recorrente	Intermitente	Rotina	Urgente	Emergência
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

5. Avaliação da Equipe SIC

Folha de Impacto de dispositivo				
Nome do Dispositivo	IP Address	P/N	N.º Série	Descrição
Folha de Impacto de software				
Nome do Software	Versão	Release	Build	Descrição
Folha de Impacto de firmware				
Hardware P/N	Versão	Release	Descrição	
Folha de Impacto de outro SIC				
Nome do Dispositivo	IP Address	P/N	N.º de Série	Descrição
Folha de documentação do impacto				
Nome do Documento	Versão	EPR	Nº de Cópias	Descrição
NOME	Data de Receção	Tipo de Mudança	Avaliação	Assinatura
Administrador do Sistema				
Oficial de Segurança SIC				

6. Controlo de Configuração

Controlo de alterações de configurações	N/A	Não	Sim	Detalhes
A mudança proposta foi aceite pela equipa SIC?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A solução final foi aceite pelos utilizadores?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Foi desenvolvido um plano de implementação pela equipa SIC?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
O plano de implementação desenvolvido pela equipa SIC inclui calendário para alcançar a solução final?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
O plano de implementação desenvolvido pela equipa SIC inclui testes prévios da solução final?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Os testes prévios da solução final são feitos com o registo dos utilizadores?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A <i>baseline</i> do DCIas vai ser alterada (BL nr.)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Os elementos de segurança do DCIas vão ser alterados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Foram identificados todos os dispositivos a ser alterados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Foram identificadas todas as interfaces, aplicações <i>middleware</i> e sistemas operativos do utilizador que vão ser alterados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Existe documentação de suporte a ser alterada?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Existem novos requisitos de treino dos utilizadores associados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Existem novos requisitos de treino dos administradores associados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Isto é, regra geral, um pedido de alteração secundária?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Isto é, regra geral, um pedido de alteração normal?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Isto é, regra geral, um pedido de alteração principal?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
O CISP ou o CISOA foi informado?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Anexo H – Formulário de Pedido de Gravação de Dados

PEDIDO DE GRAVAÇÃO DE DADOS DO DCLAS		
PARTE I: REQUERENTE		
1. NOME	2. POSTO	3. NIM
4. U/E/O	5. SUBUNIDADE	6. TELEFONE
7. CLASSIFICAÇÃO GERAL DOS DADOS A SEREM GRAVADOS	8. DATA SUBMISSÃO	9. DATA SUSPENSÃO
10. IDENTIFICAÇÃO DA(S) PASTA(S) E/OU FICHEIRO(S) A SER(EM) GRAVADO(S) (<i>FULL PATHNAME</i>): a. b. c. d.		
11. JUSTIFICAÇÃO		
12. ASSINATURA		
PARTE II: A SER APROVADO PELO COMANDANTE / DIRECTOR / CHEFE		
13. NOME	14. U/E/O	
15. APROVAÇÃO <input type="checkbox"/> SIM <input type="checkbox"/> NÃO	16. ASSINATURA	17. DATA
PARTE III: ADMINISTRADOR DO DCLAS		
18. NÚMERO DE CONTROLO DO PEDIDO DE GRAVAÇÃO DE DADOS: _____ / _____		
19. DATA DE RECEPÇÃO	20. AÇÃO POR (NOME E POSTO)	21. ASSINATURA
22. DATA DE ADMIN SISTEMA	23. AÇÃO POR (NOME E POSTO)	24. ASSINATURA
PARTE IV: REGISTO, PROCESSAMENTO E CONTROLO		
25. DATA DE RECEPÇÃO	26. AÇÃO POR (NOME E POSTO)	27. ASSINATURA
28. DATA DE DISTRIBUIÇÃO	29. AÇÃO POR (NOME E POSTO)	30. ASSINATURA
31. DATA DE ENTREGA EM MÃO AO REQUERENTE	32. NOME E POSTO	33. ASSINATURA

Página intencionalmente em branco

Anexo I – Controlo das Impressões em Papel

[illegible]

Página intencionalmente em branco

Anexo J – Administração da Segurança: Listagem de Pontos de Contacto

Service Desk

Centro de Transmissões do Exército (CTE)

Telf: 421060 / 218117053

E-mail (*unclass*): cte.apoio@exercito.pt

Website: <https://portal.rsexercito.local>

Ticketing: <http://10.172.248.11/qlpi>

Funciona em horário normal: 09h-17h. Para situações urgentes contactar o graduado de serviço à Sala de Operações CSI do CTE, telefone 421111 / 913283671.

Administrador do Sistema (System Administrator – SA)

Centro de Transmissões do Exército (CTE)

Telf: 421190

E-mail (*unclass*): cte.apoio@exercito.pt

MMHS: SUPERVISORTERRA

Oficial de Segurança do SIC (CIS Security Officer – CISSO)

Centro de Guerra de Informação e Ciberespaço (CGIC)

Telf: 421231

Email (*unclass*): cgic@exercito.pt

MMHS: CGICTERRA

LSA / LCISSE para cada site

SITE (UNIDADE)	FUNÇÃO	POSTO	NIM	NOME
EME	LSA			
	LCISSE			
CFT	LSA			
	LCISSE			
	LSA - Adj			
CSMIE	LSA			
	LCISSE			
BrigMec	LSA			
	LCISSE			
	LSA – Adj			
BrigRR	LSA			
	LCISSE			
BrigInt	LSA			
	LCISSE			
CmdPess	LSA			
	LCISSE			

Nota:

Esta listagem de Pontos de Contacto é preenchida/atualizada anualmente, ou sempre que ocorra mudança de pessoal, pelo CISO, conforme responsabilidade atribuída e dispensando promulgação de outros anexos.

Data:

O CISO, assinatura

Anexo K – Registo de Alterações dos SecOPs

[illegible]

Página intencionalmente em branco

Domínio Classificado da Rede de Dados do Exército

PROCEDIMENTOS DE OPERAÇÃO DE SEGURANÇA (SecOPs)

Versão 1.0

20 de março de 2024

Direção de Comunicações e Informação

