

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

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.