NT – E 08
01DEZ2020

Gabinete Nacional de Segurança
PORTUGAL

NORMA TÉCNICA – E 08

SISTEMA DE SEGURANÇA ELETRÓNICA DA INFORMAÇÃO (SEIF).

Lisboa, 01 de dezembro de 2020

A Autoridade Nacional de Segurança

António José Gameiro Marques

Digitally signed by António José Gameiro Marques
Date: 2020.12.04 08:56:43 Z

(António Gameiro Marques)

(Verso em branco)

(ESTA PÁGINA FOI DEIXADA EM BRANCO INTENCIONALMENTE)

1. REFERÊNCIAS

a. Resolução do Conselho de Ministros n.º 50/88, de 8 de setembro (SEGNAC 1);

b. C-M (2002)49 – *Security Within NATO*;

c. AC/35-D/2002 – *Directive on Security of Information*;

d. AC/35-D/1037 – *Supporting Document for the Security of Electronic Registry Systems*;

e. ESA/REG/004 – *Security Regulations of the European Space Agency*, 18 de janeiro 2012.

f. Decisão nº2013/488 - *do Conselho, de 23 de setembro, relativa às regras de segurança aplicáveis à Proteção das Informações Classificadas da UE*.

2. SITUAÇÃO

A aplicação designada por Segurança Eletrónica da Informação (SEIF) foi desenvolvida conforme requisitos do Gabinete Nacional de Segurança (GNS). O conjunto de equipamentos informáticos, no qual é instalado ou disponibilizado o SEIF, dispositivo de segurança de rede, impressora e digitalizador de documentos é designado por Sistema SEIF. Este sistema, em funcionamento desde 2001, destina-se a ser disponibilizado a órgãos de segurança (Registo Central, Sub-Registos e Postos de Controlo) no Continente, Regiões Autónomas dos Açores e Madeira, e nas representações Nacionais no estrangeiro. O Sistema SEIF interliga diversos órgãos de segurança das Forças Armadas, Forças de Segurança e todo um conjunto de Organismos Estatais. Assegura também a ligação às Delegações e Missões Militares junto da Organização do Tratado do Atlântico Norte (NATO) e União Europeia (UE).

3. OBJETO/FINALIDADE

Dada a importância do Sistema SEIF para gestão e transferência da Informação Classificada (IC) das marcas NACIONAL, NATO, UE e da Agência Espacial Europeia (ESA) ou de outras para o qual venha a ser acreditado, importa definir objetivamente os requisitos para instalação, acesso, operação e manutenção.

4. ÂMBITO

A presente norma destina-se a ser do conhecimento de todos os Chefes de Órgãos de Segurança que se encontram equipados com o Sistema SEIF.

5. EXECUÇÃO

a. Características do Sistema SEIF.

(1) O SEIF é o sistema de gestão documental atualmente implementado e utilizado pela generalidade dos órgãos que integram a Estrutura Nacional de Segurança para Gestão da IC;

(2) O SEIF permite a gestão de registos de informação classificada NACIONAL, NATO, UE e ESA até ao grau de segurança SECRETO e equivalente, permitindo ainda a transferência de informação classificada em formato eletrónico;

(3) A sua arquitetura tem como referência os princípios de uma relação hierárquica entre organizações e de uma relação funcional dos órgãos, estando no topo a entidade responsável pelo sistema, o Registo Central (RC);

(4) A utilização do Sistema SEIF destina-se exclusivamente ao descrito em (2), não sendo permitido a sua exploração para outros fins.

b. Perfis de Acesso.

O acesso às diferentes funcionalidades do SEIF tem como base perfis de acesso, com privilégios de utilização previamente estabelecidos e a seguinte política de atribuição:

(1) Administrador de Sistema (ADMIN CISP)

Perfil atribuído ao responsável pela gestão do sistema. Este perfil é atribuído unicamente aos elementos do *Communications and Information System Provider* (CISP) responsáveis pela instalação, configuração e gestão de toda a infraestrutura tecnológica que suporta o SEIF, incluindo os *endpoints*.

Este perfil permite:

(a) Instalar, configurar e desinstalar *software* e *hardware*;

(b) Configuração de *network*;

(c) Gestão dos perfis de acesso ao ambiente operativo;

(d) Configurações de segurança;

i. Encriptação do disco;

ii. Gestão da firewall;

iii. Gestão de antivírus e *anti-malware*.

(e) Configuração de firewall e rede.

(2) Auditor de Sistemas (CISO)

Perfil atribuído ao Responsável de Segurança de Informação, designado por *Chief Information Security Officer* (CISO).

Este perfil permite:

(a) Verificar a eficácia dos controlos e procedimentos de segurança existentes, a eficiência dos processos em uso e a correta utilização dos recursos disponíveis.

(b) Monitorizar os arquivos de atividades e registo de eventos para auditoria.

(c) Privilégios para de forma simples e automática customizar a seleção dos campos e/ou registos a observar.

(3) Administrador Aplicacional (ADMIN CISOA).

Perfil atribuído ao Chefe do RC, responsável pela gestão aplicacional do sistema, designado por *Comunication and Information System Operational Authority* (CISOA). Por delegação, este perfil é atribuído unicamente aos elementos do RC responsáveis pela operação e parametrização do sistema. Permite, além das funcionalidades de administrador local e operador:

(a) Parametrizar o SEIF;

(b) Gerir destinatários para distribuição de informação;

(c) Gerir utilizadores e acesso aplicacional;

(d) Gerir perfis de acesso aplicacional;

(e) Apoio aplicacional aos utilizadores;

(f) Formação aplicacional.

(4) Administrador Local Aplicacional.

Perfil atribuído ao responsável pelo órgão de segurança no qual se encontra instalado o Sistema SEIF. Este perfil permite a gestão de acessos e eventuais alterações a serem introduzidas, além das funcionalidades de operador:

(a) Gestão de senhas de acesso;

(b) Gestão de privilégios a operadores;

(c) Bloquear acessos.

(5) Operador.

Perfil atribuído a utilizadores que desempenhem funções de operação no órgão de segurança no qual o Sistema SEIF se encontra instalado. Permite registar, distribuir, arquivar e destruir registos e informação de acordo com a parametrização efetuada pelo Administrador Local.

(6) Consulta.

Perfil atribuído a pessoal a desempenhar funções no organismo no qual o SEIF se encontra instalado. Permite apenas consultar a informação em formato eletrónico da marca e grau para a qual está credenciado e autorizado.

c. Requisitos de Instalação.

(1) O Sistema SEIF é instalado nos Órgãos de Segurança, a seu pedido ou por proposta do GNS e quando satisfeito um conjunto de requisitos no âmbito da Segurança Física, Segurança Eletrónica Segurança do Pessoal;

(2) A instalação carece de uma inspeção de segurança por parte do GNS a fim de acreditar a mesma e assegurar que os seguintes requisitos são cumpridos:

(a) O *hardware* será instalado numa Área de Segurança de Classe 1;

(b) O Órgão dispõe da uma rede de comunicações;

(c) Existem contentores de segurança específicos para guarda de chaves e códigos de acesso à área, eventuais *back-ups*, *software*, informações classificadas e ou códigos de acesso ao sistema;

(d) O acesso à área onde se encontra instalado o Sistema SEIF é apenas permitido ao pessoal autorizado e constante na respetiva Lista de Acesso ao local;

(3) Após acreditadas as instalações, o Órgão que pretende a instalação do Sistema SEIF deve enviar ao RC do GNS:

(a) A identificação do Administrador Local do Sistema SEIF e os pedidos de acesso ao sistema, indicando o perfil pretendido (Operador ou Consulta) (Anexo A).

(b) A lista de destinatários de informação com os quais o órgão se relaciona.

I. Esta lista será composta pelos órgãos e entidades da estrutura funcional e hierárquica na qual o órgão está inserido;

ii. Não são permitidos destinatários sobre os quais não exista a absoluta certeza da sua habilitação de segurança, autorização de acesso e necessidade de conhecer a informação;

iii. Não é permitida a utilização de nomes pessoais como destinatários de informação.

(c) Estas informações deverão ser atualizadas sempre que sofram alteração.

(4) O Registo Central deve:

(a) Verificar se o Administrador Local e Operador(es) são detentores de habilitação de segurança válida, na marca e grau da informação que vão manusear assim como o curso de formação de operador do Sistema SEIF;

(b) Caso não possuam formação de operador, excecionalmente, poderá ser dispensado este requisito mediante a inscrição na próxima ação de formação a realizar pelo GNS;

(c) Verificadas as condições previstas nas alíneas (a) e (b), criar uma conta para cada utilizador atribuindo um nome de utilizador, perfil de acesso e senha para cada domínio (Marca de Segurança);

(d) Criar a lista de entidades destinatárias de informação do órgão.

d. Instalação do Sistema SEIF.

(1) Os equipamentos informáticos, com a aplicação SEIF instalada, são distribuídos pelo GNS e estão sujeitos a exigências de segurança idênticas às consideradas para as informações classificadas;

(2) Não é permitida a instalação ou desinstalação de *hardware* no interior do sistema fornecido pelo GNS nem a violação dos selos apostos nos mesmos;

(3) O Sistema Operativo está configurado de forma a impedir a instalação ou desativação de *software*;

(4) A instalação do Sistema SEIF nos Órgãos de Segurança envolve a preparação, a configuração e o teste do sistema, por forma a garantir a sua operacionalidade em termos de exploração e, ainda, formação local dos utilizadores, que é complementada com cursos a ministrar posteriormente;

(5) Após a instalação do sistema não é permitida a sua movimentação para outras instalações, mesmo dentro do mesmo edifício, sem que as mesmas sejam acreditadas pelo GNS;

(6) O equipamento não pode ser instalado a menos de um metro de distância de telefones, outros dispositivos de comunicações ou qualquer outro equipamento elétrico de processamento de informações classificadas;

(7) Eventuais visitantes que não possuam uma habilitação de segurança ou necessidade de conhecer e que necessitem de aceder ao local onde se encontra instalado o Sistema SEIF deverão ser, permanentemente, acompanhados em conformidade com as normas de segurança em vigor.

e. Operação do SEIF.

(1) Conceitos Gerais.

(a) Os equipamentos instalados não podem ser utilizados para fins diferentes dos relacionados com o SEIF;

(b) Os equipamentos devem estar identificados com a Marca e a máxima classificação de segurança da informação que é permitido processar;

(c) Qualquer falha de *hardware* deve ser de imediato comunicada ao RC como primeira entidade / 1° escalão;

(d) Após autenticação do utilizador, este pode aceder ao SEIF e a todas as funcionalidades que o seu perfil permita;

(e) Não é permitida a partilha de credenciais de acesso entre diferentes utilizadores;

(f) Não é permitida a ligação aos equipamentos de qualquer tipo de sistemas (pessoais ou institucionais) não autorizados pelo GNS;

(g) Quando os utilizadores se ausentarem do posto de trabalho devem bloquear o sistema ou terminar a sessão;

(h) O servidor e a unidade de alimentação ininterrupta (*Uninterruptible Power Supply – UPS*) não devem ser desligados;

(i) Os utilizadores devem estar cientes de que em caso de falha mecânica a informação pode ficar armazenada em memória (incluindo impressoras), se não forem tomadas medidas de limpeza depois de concluída a operação;

(j) O acesso não autorizado ao sistema ou a alteração das suas características constitui uma quebra de segurança.

(2) Acesso ao Sistema.

(a) O processo de Identificação e Autenticação (I&A) dos utilizadores consiste no acesso ao servidor/terminal do órgão onde estão criadas as contas. O controlo para efeitos de I&A no acesso ao SEIF consiste:

i. Domínio.

Seleção do domínio pretendido (NACIONAL, NATO, EU ou ESA). Os domínios são atribuídos ao Órgão pelo RC de acordo com o processo de acreditação de segurança;

ii. Utilizador.

Introdução do nome de utilizador. O nome de utilizador atribuído a cada utilizador é criado pelo RC segundo a regra:

- Carateres em maiúsculas;
- Primeira letra do nome e apelido.

iii. Senha.

Introdução da senha individual. Quando atribuído um nome de utilizador é atribuída, também, uma senha cuja política de utilização deverá ser a seguinte:

- O utilizador, no primeiro acesso ao SEIF, em cada domínio, é responsável por alterar a senha que lhe foi atribuída;
- A senha do utilizador é pessoal, intransmissível e deve ser memorizada, não devendo estar escrita por forma a negar a sua utilização por indivíduos não autorizados;
- Os Administradores Locais são responsáveis pela gestão de senhas e devem assegurar-se que as mesmas são alteradas periodicamente, idealmente todos os meses.

(b) O período de acesso ao sistema só é atribuído de acordo com a habilitação de segurança do utilizador.

(c) Cada utilizador apenas pode aceder a um sistema. Um pedido de acesso substitui automaticamente outro, anteriormente formulado.

(3) Processamento de Informação.

(a) O SEIF destina-se à gestão de toda a informação classificada de acordo com a Norma Técnica - E 01 "MARCAS, GRAUS DE SEGURANÇA E DESIGNADORES", permitindo:

i. A gestão documental de IC, conforme descrito anteriormente;

ii. Também é permitida a sua utilização na gestão e transferência de informação não classificada.

(b) O SEIF não deve ser utilizado para gestão e transferência de informação sensível como o Segredo de Estado, informações referentes a dados pessoais e sigilosas do âmbito jurídico, médico e comercial, protegidas por legislação própria ou ética profissional;

(c) Não são autorizados no SEIF registos de dados que identifiquem ou tornem identificável um indivíduo (exemplo: nome, número de identificação, morada, etc.);

(d) Os processos de credenciação são registados sem que conste nos registos os elementos referidos no ponto anterior;

(e) Manuseamento da Informação.

i. A informação que se encontra em formato eletrónico no SEIF deve ser consultada, na aplicação, através da função 'Visualização de Exemplares' do menu 'Distribuição';

ii. Quando necessário, passar a informação em formato eletrónico para suportes informáticos, físicos, (DVD, CD, etc.) através da função 'Extração de Exemplares' do menu 'Distribuição'. O operador tem a responsabilidade de identificar os suportes informáticos com a Marca e a mais alta classificação de segurança da informação neles contida como o número de registo de controlo, exemplar e cópia da informação;

iii. Não é permitido o armazenamento de informação de diferentes Marcas num mesmo suporte informático externo;

iv. Não é permitida a extração de informação em formato eletrónico para pastas ou qualquer outro destino do equipamento que não seja o atrás referido;

v. A utilização de suportes informáticos, físicos (DVD, CD, *Pen Drive*, etc.), para manusear informação carece de autorização especial por parte do RC e da implementação de procedimentos de segurança específicos para este tipo de suportes;

vi. Imprimir, quando estritamente necessário, a informação em formato eletrónico, ou partes da informação, através da função 'Impressão de Exemplares' do menu 'Distribuição';

vii. Registar todas as cópias de informação que seja necessário efetuar;

viii. Arquivar no SEIF, se possível, toda a informação que se encontre em formato eletrónico através da função 'Arquivar' do menu 'Arquivo';

ix. A distribuição de informação é sempre efetuada mediante a emissão de Guia de Transferência a fim de ser assinada pelo destinatário. A transferência de informação em formato eletrónico não carece da impressão de Guia de Transferência e como tal, não é necessário o seu envio ao destinatário para assinar;

x. Destruir a informação desnecessária, repetida ou obsoleta, através das funções do menu 'Destruição' e emitir o respetivo Certificado.

(4) Distribuição de Informação.

Só é permitida a distribuição de informação aos órgãos e entidade previstos na lista de distribuição (5.c.(3)(b)) e aos órgãos de segurança que se encontram ao seu nível na mesma dependência funcional. Não é permitido aos Órgãos corresponderem-se com entidades externas à Estrutura Nacional de Segurança para Gestão da IC implementada.

(5) Gestão de Auditorias.

Os eventos gerados no SEIF incluem entre outros: a hora, a data, o tipo e a identificação do utilizador.

f. Manutenção do Sistema SEIF.

(1) A manutenção do SEIF é da responsabilidade do GNS, pelo que todas as anomalias que venham a ser detetadas deverão ser reportadas, pelo canal técnico, a este Gabinete. Para este efeito deverá ser usado o impresso que se junta em Anexo B;

(2) A resolução das anomalias verificadas no Sistema, será efetuada remotamente, se tal for possível, ou sendo necessário, pelo GNS que procederá à sua reparação no local. Caso esta não seja viável, poderá ser solicitado o envio do equipamento para o GNS, cumprindo os requisitos idênticos a uma transferência de IC;

(3) Os custos decorrentes das reparações ou substituições serão suportados pelas estruturas apoiadas pelo correspondente Órgão de Segurança;

(4) A partir da instalação inicial, qualquer avaria que surja nos equipamentos periféricos (monitor, teclado, rato, impressora, digitalizador e UPS) que venha a implicar a sua substituição, deverá ser efetuada pelas estruturas apoiadas pelos correspondentes Órgãos de Segurança sob supervisão técnica deste Gabinete;

(5) Para o caso específico do equipamento servidor ou terminal e dado que contêm informação classificada, não só a aplicação SEIF como também a residente nos discos que são considerados classificados, a sua substituição será efetuada exclusivamente pelo GNS.

g. Responsabilidades.

Os chefes dos órgãos de segurança nos quais se encontra instalado o Sistema SEIF são responsáveis pela correta operação do sistema, medidas locais de segurança e reporte ao GNS de qualquer anomalia verificada.

h. Encerramento de órgãos de segurança.

Só é permitido o encerramento de um órgão equipado com o Sistema SEIF após toda a informação arquivada e distribuída, a entidades sob a sua responsabilidade, ser destruída ou redistribuída a outro órgão de segurança.

6. DIVERSOS

Nada a referir.

7. ACRÓNIMOS

CD - *Compact Disc*
CISO - *Chief Information Security Officer*
CISOA - *Communications and Information System Operational Authority*
CISP - *Communications and Information System Provider*
CPU - *Central Processing Unit*
DVD - *Digital Video Disc*
ESA - *European Space Agency*
GNS - Gabinete Nacional de Segurança
I&A - Identificação e Autenticação
IC - Informação Classificada
NATO - *North Atlantic Treaty Organization*
RC - Registo Central
SEIF - Segurança Eletrónica da informação
UE - União Europeia
UPS - *Uninterruptible Power Supply*

8. ANEXOS

Anexo A – Acesso ao Sistema de Segurança Eletrónica da Informação (SEIF).

Anexo B – Pedido de Intervenção no SEIF.

ACESSO AO SISTEMA DE SEGURANÇA ELETRÓNICA DA INFORMAÇÃO (SEIF)

Declaro que tomei conhecimento das normas para o acesso e manuseamento da informação classificada no Sistema de Segurança Eletrónica da Informação (Sistema SEIF), do _____[(1)] e especificamente no que respeita à:

a) Criação, eliminação e alteração de registos e/ou informação na aplicação;

b) Procedimentos de gravação e importação de ficheiros de e para o sistema informático, via suportes externos;

c) Procedimentos para a impressão de informação e extração de ficheiros da aplicação;

d) Proibição de retirar informação classificada sem que seja controlada.

(Local e data) _____, _____ de _____ de _____

(Assinatura) _____

_____

(Posto ou categoria)

[(2)] Nos termos da legislação em vigor, consinto de forma livre, específica e inequívoca que o Gabinete Nacional de Segurança proceda à recolha dos meus dados pessoais, com finalidade de gestão, organização e análise estatística no contexto de acesso ao Sistema SEIF.

(1) Designação do Órgão de Segurança
(2) Preencher com ✕.

ACESSO AO SISTEMA DE SEGURANÇA ELETRÓNICA DA INFORMAÇÃO (SEIF)

Data do Pedido	

ÓRGÃO DE SEGURANÇA

CHEFE DIRETO			
Nome Completo			
Posto/Categoria		NIM/CC	
Contacto		E-MAIL	

Declaro que o requerente tem necessidade efetiva, para desempenho das suas funções ou tarefas, de aceder/operar o Sistema SEIF.

(Assinatura) _____

_____

REQUERENTE			
Nome Completo			
Posto/Categoria		NIM/CC	
Função			
Contacto		E-MAIL	

PERFIL DE ACESSO REQUERIDO	
Perfil	Observações

HABILITAÇÃO DE SEGURANÇA				
Marca	Grau	Certificado	Validade	Observações
NACIONAL				
NATO				
UE				
ESA				

AUTORIZAÇÃO E ACESSO (A PREENCHER PELO REGISTO CENTRAL)				
Função	Nome	Posto/Categoria	Data	Assinatura

Perfil Atribuído	
Utilizador	

Data de Conclusão do Pedido	

PEDIDO DE INTERVENÇÃO NO SEIF

1. **Identificação**
   Órgão de Segurança:
   Número de Pedido:
   Operador:
   Data:

2. **Descrição do Pedido:**

Instruções de Preenchimento

1. O formulário de Pedido de Intervenção no SEIF deve ser utilizado sempre que necessite de assistência técnica do Registo Central para a operação, configuração ou gestão do sistema. Isto inclui as seguintes situações:

   a. Relato de erro na aplicação ou anomalia de equipamento;

   b. Incidente de segurança;

   c. Configuração de novo dispositivo (impressora, digitalizador ou outro);

   d. Adição, remoção ou alteração de designação de entidades subordinadas;

   e. Gestão de utilizadores, como desativação ou renovação de senha de acesso em caso de esquecimento.

2. Se possível, preencha este formulário em formato digital, usando um processador de texto.

3. Em caso de pedido de intervenção, descreva pormenorizadamente o tipo de intervenção de que necessita.

4. Em caso de anomalia, inclua a descrição da operação que tentou efetuar, as eventuais mensagens de erro obtidas e as páginas onde se registaram. Se for viável, e caso não incluam informação classificada, anexe também capturas de ecrã dos erros obtidos e/ou passos efetuados.

5. Para sua segurança, após terminar o preenchimento pode assinar o documento digitalmente com o cartão de cidadão, quer em formato editável (processador de texto) ou não editável (PDF). Com o documento assinado digitalmente assegura-se de que este não será alterado após o envio.

6. Envie o pedido por correio eletrónico para o Registo Central (seif@gns.gov.pt), tratando-se de um Sub-Registo, ou através do Sub-Registo do qual depende, se for um Posto de Controlo. No assunto, coloque: "Pedido de intervenção SEIF: *ENTIDADE – ano/número*".