c. ATO NORMATIVO – Publicação

ORIENTAÇÃO NORMATIVA Nº 05/CMT LOG HFA, DE 15 DE AGOSTO DE 2019.

Dispõe sobre a Política de Segurança da Informação e Comunicações do Hospital das Forças Armadas (POSIC/HFA).

O Comandante Logístico do Hospital das Forças Armadas, no uso da atribuição que lhe é conferida pelo inciso I do artigo 35° do Regimento Interno do HFA, aprovado pela Portaria Normativa n° 10/MD, de 7 de Março de 2018, do Ministro da Defesa, e tendo em vista a Portaria Normativa nº 559/MD, de 3 de maio de 2005, do Ministro da Defesa, resolve:

Art. 1º Instituir, no âmbito do Hospital das Forças Armadas (HFA), a Política de Segurança da Informação e Comunicações do HFA (POSIC/HFA), regida pelos objetivos e diretrizes estabelecidas nesta Orientação Normativa.

1. DO ESCOPO

1.1 A Política de Segurança da Informação e Comunicações – PoSIC institui diretrizes, competências e responsabilidades para garantir a disponibilidade, integridade, confidencialidade e autenticidade (DICA) das informações e comunicações no Hospital das Forças Armadas.

1.2 A PoSIC trata do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do HFA, em todo o seu ciclo de vida – criação, manuseio, divulgação, armazenamento, transporte e descarte, visando, normas e procedimentos pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

1.3 As diretrizes, normas complementares, manuais e procedimentos decorrentes da PoSIC aplicam-se a servidores, militares, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas ao HFA.

2. DOS CONCEITOS

2.1 Para efeitos desta Orientação Normativa estabelece-se os significados dos seguintes termos e expressões:

a. **Ativos de Informação:** os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

b. **Ameaça:** qualquer evento que explore vulnerabilidades, ou seja, causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

c. **Assinatura Digital:** processo eletrônico de assinatura, que permite ao usuário garantir a autoria, autenticidade e a integridade de um documento;

d. **Autenticidade:** Garante a identidade de quem está enviando a informação, ou seja, gera o não repúdio que se dá quando há garantia de que o emissor não poderá se esquivar da autoria da mensagem;

e. **Análise de riscos:** uso sistemático de informações para identificar fontes e avaliar riscos;

f. **Auditoria:** é um processo que consiste em reunir, agrupar e avaliar evidências para determinar se um sistema de informação suporta adequadamente um ativo de negócio, mantendo a integridade dos dados, e realiza os objetivos esperados, utiliza eficientemente os recursos e cumpre com as regulamentações e leis estabelecidas;

g. **Comitê de Segurança da Informação e Comunicações:** grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da administração do Hospital das Forças Armadas;

h. **Confidencialidade:** propriedade que garante acesso à informação somente as pessoas autorizadas, assegurando que indivíduos, sistemas, órgãos ou entidades não autorizadas não tenham conhecimento da informação, de forma proposital ou acidental;

i. **Conformidade:** é o ato de aderir a leis e regulamentos externos, assim como as políticas e procedimentos corporativos. Controles que combinam ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), etc;

j. **Desastre:** evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais ou críticos, por um período de tempo superior ao prazo de recuperação;

l. **Dado:** é o conteúdo quantificável e que por si só não transmite nenhuma mensagem que possibilite o entendimento sobre determinada situação. Os dados podem ser considerados a unidade básica da informação;

k. **Disponibilidade:** as informações estarão disponíveis e utilizável a quem dela necessita e possua autorização para acessá-la;

m. **Equipe de tratamento e respostas a incidentes em redes de computadores – ETIR:** grupo responsável por receber, analisar e corrigir incidentes que comprometam a segurança da rede;

n. **Gestão de continuidade:** a gestão de continuidade de serviços de TI é um processo que visa reduzir desastres que afetam os serviços de TI e mantém os serviços em pleno funcionamento a fim de garantir que o negócio não sofra interrupções. A gestão de continuidade de serviços de TI é parte e depende da Gestão de continuidade de Negócios (GCN).É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas softwares, hardware, infraestrutura etc.) por ele utilizados;

o. **Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC:** conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

p. **Gestão de Segurança da Informação e Comunicações – GSIC:** coordena a integração das atividades de gestão de riscos, gestão de continuidade dos serviços de TI, tratamento de incidentes, tratamento da informação, auditoria e conformidade, segurança física, no âmbito do HFA;

q. **Gestor de Segurança da Informação e Comunicações:** responsável pelo planejamento e fiscalização das ações de proteção dos ativos de informação e comunicações;

r. **Incidente:** evento adverso, confirmado ou sob suspeitas, relacionado à segurança dos sistemas de computação ou às redes de computadores;

s. **Integridade:** propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino, representando a fidedignidade da informação;

t. **Informação:** É o resultado do processamento dos dados. Ou seja, os dados foram analisados e interpretados sob determinada ótica, e a partir dessa análise se torna possível qualificar esses dados.

u. **Resiliência:** poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

v. **Segurança da Informação e Comunicações (SIC):** ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

x. **Tratamento de incidentes:** processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências potenciais futuras;

y. **Termo de compromisso e manutenção de sigilo – TCMS (Anexo):** termo a ser assinado para autorizações especiais de acessos;

w. **Usuário:** servidores, militares, residentes, terceirizados, voluntários, consultores, estagiários ou qualquer pessoa autorizada a utilizar os ativos de informações e comunicações; e

z. **Vulnerabilidade:** fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

3. DAS REFERÊNCIAS LEGAIS E NORMATIVAS

3.1 Esta PoSIC observa a legislação e normas específicas, destacando-se:

a. Decreto nº 3.505, de 13 de junho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

b. Decreto nº 5.482, de 30 de junho de 2005 – Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Internet;

c. Decreto nº 1.171, de 22 de junho de 1994 – Aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

d. Lei 12.527, de 18 de novembro de 2011 – Regula o acesso a informações;

e. Lei 8.112, de 11 de dezembro de 1990 – Dispõe sobre o regime jurídico dos servidores da União, das Autarquias e das fundações públicas federais;

f. Lei nº 9.983, de 14 de julho de 2000 – dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

g. Resolução do Conselho Federal de Medicina nº 1931/2009 – Código de Ética Médica;

h. Regulamentos Disciplinares da Marinha, do Exército e da Força Aérea Brasileira;

i. NBR ISO-IEC 27001 – Gestão de Segurança da Informação – Requisitos;

j. NBR ISO-IEC 27002 – Gestão de Segurança Informação; e

k. NBR ISO-IEC 27005 – Gestão de Riscos de Segurança Informação.

l. Instrução Normativa GSI 01, de 13 de junho de 2008;

m. NC 03/IN01/DSIC/GSIPR – Diretrizes para elaboração da PoSIC; e

n. Normas Complementares 01, 02, 03, 04, 05, 06, 07, 08, 11, 12, 14, 15, 19 e 20 da IN01/DSIC/GSIPR, de 13 de outubro de 2008.

4. DOS PRINCÍPIOS

4.1 Esta PoSIC observa os seguintes princípios, assim definidos:

a. Responsabilidade: os agentes públicos (servidores, militares, residentes, terceirizados, voluntários, consultores, estagiários) devem conhecer e respeitar a POSIC do HFA;

b. Ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da segurança da informação e comunicações;

c. Clareza: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

d. Legalidade: as ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais da HFA;

e. Publicidade: transparência no trato da informação, observados os critérios legais; e

f. Privilégio: permissão a usuários para acesso somente aos ativos de informação necessários para realizar suas respectivas atividades.

5. DAS DIRETRIZES GERAIS

5.1 Da Gestão de Segurança da Informação e Comunicações – GSIC

5.1.1 Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade dos serviços de TI.

5.1.2 De forma a promover a gestão e fomentar os aspectos de segurança da informação, a **DTI –** Divisão de Tecnologia da Informação, no âmbito da rede corporativa do HFA, deve:

a. Instituir uma estrutura para a gestão de segurança da informação e comunicações;

b. Nomear um gestor de segurança da informação e comunicações; e

c. Instituir/possuir uma **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**, apta a identificar e tratar os incidentes que comprometam a segurança da informação e comunicações.

5.2. Do Tratamento da Informação

5.2.1 As informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e *legislação específica em vigor.*

5.2.2 Todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

5.2.3 Toda informação institucional, se eletrônica, estará armazenada nos servidores de arquivo e bases de dados sob gestão e administração da área de TIC e, se não eletrônica, mantida em local que a salvaguarde adequadamente.

5.2.4 Para garantir um local na rede de fácil utilização existe um diretório público. Este não deverá ser utilizado para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível. Esse diretório também não deve ser utilizado como local de armazenamento permanente, pois todos os usuários têm acesso, não está incluída na rotina do backup e será limpo semanalmente.

5.3 Do Tratamento de Incidentes de Rede

5.3.1 Cabe à DTI – Divisão de Tecnologia da Informação do HFA manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

5.4 Da Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)

5.4.1 A Gestão de Riscos de Segurança da Informação e Comunicações fica estabelecida com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações.

5.4.2 Os riscos devem ser analisados, identificados e continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco.

5.5 Da Gestão de Continuidade

5.5.1 A Gestão de Continuidade prevê a definição de uma estrutura para que se aprimore a resiliência organizacional, com vistas a responder efetivamente aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do HFA, além de recuperar perdas de ativos de informação.

a. A DTI deverá manter um processo de gestão de continuidade de serviços de TI, de modo a não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos, e também assegurar a sua retomada em tempo hábil, quando for o caso.

5.6 Da Auditoria e Conformidade

5.6.1 A DTI no âmbito da rede corporativa do HFA deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna do HFA.

5.6.2 Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das melhores práticas de *SIC* do HFA com esta PoSIC e procedimentos complementares, bem como com a legislação específica em vigor.

5.6.3 A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos dos mesmos gêneros celebrados com a administração do HFA.

5.7 Dos Controles de Acesso

5.7.1 O controle de acesso às instalações e informações, o credenciamento de acesso de usuários aos ativos de informação, e aos recursos computacionais do HFA, ou sob sua guarda considerados críticos, devem ser implantados nos níveis físico e lógico e serão definidos em norma específica, em conformidade com as diretrizes desta POSIC. É proibido também aos usuários habilitar o acesso remoto em qualquer equipamento ou computador sem a autorização da DTI. Acompanhado a esses controles, o ***Termo de Compromisso e Manutenção de sigilo – TCMS***, responsabilizando-se pela confidencialidade, integridade e disponibilidade das informações, a que tiverem acesso deve ser assinado.

5.8 Do Uso da Internet e Intranet

5.8.1 O acesso à rede de computadores (Internet), bem como a Intranet, e a utilização de comunicadores (ex: Skype e googletalk), redes sociais (ex: Facebook e Instagram), bem como download de arquivos grandes (superior a 100 Mb), no âmbito do HFA, será regido por norma interna, em conformidade com as diretrizes desta PoSIC, orientações governamentais e legislações específicas em vigor.

5.9 Do Uso do Correio Eletrônico (e-mail)

5.9.1 O uso do e-mail corporativo no âmbito do HFA deve ser definido em norma específica, em conformidade com as diretrizes desta POSIC, e deve tratar, dentre outras coisas, do controle de acesso.

5.10 Do Inventário e Mapeamento de Ativos de Informação

5.10.1 O processo de inventário dos ativos de informação deverá ser periódico e estruturado de modo a otimizar e controlar todos os recursos.

5.11 Dos Dispositivos Móveis

5.11.1 O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito do HFA deve ser controlado, com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, de acordo com procedimentos definidos em norma específica e em conformidade com as diretrizes desta PoSIC.

a. Todo dispositivo móvel usado para acessar a rede corporativa do HFA estará submetido aos padrões estabelecidos pela DTI; e

b. A DTI proverá uma rede segregada da rede corporativa para acesso à Internet pelos visitantes.

5.12 Das Contratações, Convênios, Acordos de Serviços

5.12.1 Nos editais de licitação e contratos de empresas prestadoras de serviços firmados com o HFA deverá constar cláusulas que assegurem a manutenção do sigilo e a segurança da informação e comunicações, bem como, ser exigida da empresa contratada a assinatura do ***TCMS*** (Anexo).

6. DAS COMPETÊNCIAS E RESPONSABILIDADES

6.1. Ao Comitê de Segurança da Informação e Comunicações compete:

a. atualizar a POSIC; e

b. propor, analisar e aprovar normas complementares relativas à segurança da informação e comunicações, em conformidade com as legislações vigentes sobre o tema.

6.2. À Divisão de Tecnologia da Informação do HFA – DTI compete:

a. planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC em conformidade com as diretrizes desta POSIC;

b. elaborar, implementar e atualizar normas internas específicas em conformidade com esta POSIC e demais diretrizes do Governo; e

c. manter uma área de Segurança da Informação e Comunicações com a responsabilidade de apoiar o Gestor de Segurança da Informação e Comunicações no cumprimento de suas atribuições.

6.3. Ao Gestor de Segurança da Informação e Comunicações compete:

a. promover cultura de segurança da informação e comunicações;

b. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c. Verificar se os procedimentos de Segurança da Informação e Comunicações (SIC) estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativas internas específicas;

d. Gerenciar a análise de risco; e

e. acompanhar a Equipe de Tratamento e Resposta a Incidentes em redes computacionais.

6.4. Às Chefias em todos os níveis compete:

a. Divulgar, cumprir e fazer cumprir esta Política e as demais normas e procedimentos relativos à Segurança da Informação e Comunicações;

b. Comunicar imediatamente, ao Comitê de Gestão de Tecnologia da Informação, eventuais casos de violação da PoSIC; e

c. A Seção de Divisão de Pessoal civil e militar deverá lavrar os Termos de Compromisso e Manutenção do Sigilo de todos os militares, servidores e funcionários civis, residentes, estagiários e empregados de empresas terceirizadas, e mantê-los arquivados, de acordo com o Decreto nº 4.553, de 27 dez 2002.

6.5. À Equipe de tratamento e respostas a incidentes em redes computacionais – ETIR compete:

a. Avaliar a segurança da rede de computadores, propor e implementar medidas;

b. Coordenar as atividades de respostas a incidentes de rede e recuperação de sistemas; e

c. Em caso de indisponibilidade de algum recurso de rede, substituir o recurso, considerando a necessidade do setor, a disponibilidade de recursos sobressalentes.

6.6. À Divisão de Recursos Humanos compete:

a. Comunicar a DTI o desligamento de pessoal civil e militar via e-mail ou protocolo eletrônico; e

b. Promover a ambientação, conhecimento e treinamento das responsabilidades de SIC aos chefes e servidores na assunção dos cargos ou em treinamentos eventuais do pessoal.

6.7. Aos Usuários compete:

a. Acessar a rede de dados do HFA somente após tomar ciência das normas de *SIC* e assinar o ***TCMS,*** bem como, feito seu credenciamento de acesso;

b. Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do HFA exclusivamente para o interesse do serviço; e

c. Utilizar sempre seu próprio usuário (***login***) e senha, e jamais repassá-lo a terceiros.

7. DA DIVULGAÇÃO

7.1. A POSIC e as normas deverão ser divulgadas no boletim interno do HFA e disponibilizadas na Intranet para todos os militares, servidores e funcionários civis, residentes, estagiários e empregados de empresas terceirizadas.

7.2 A DTI deverá promover ações permanentes de conscientização visando à disseminação das diretrizes e normas estabelecidas nesta política.

8. DA ATUALIZAÇÃO E VIGÊNCIA

8.1. Esta POSIC/HFA e todos os instrumentos normativos gerados a partir dela devem ser revisados sempre que se fizer necessário, não devendo exceder o período máximo de 2 (dois) anos.

9. DAS PENALIDADES

9.1. Os servidores militares e civis do HFA poderão responder administrativa, civil ou penalmente pelas ações e omissões que possam pôr em risco uma ou mais regras previstas nesta POSIC, de acordo com a legislação em vigor.

Art. 2º Esta Orientação Normativa entra em vigor na data de sua publicação.

(a) Gen Div RUY YUTAKA MATSUDA
Comandante Logístico do Hospital das Forças Armadas

ANEXO
TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO (TCMS)

MINISTÉRIO DA DEFESA
SECRETARIA-GERAL
SECRETARIA DE PESSOAL, ENSINO, SAÚDE E DESPORTO
HOSPITAL DAS FORÇAS ARMADAS
DIVISÃO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO (TCMS)
(Decreto nº 7,845, de 14 de novembro de 2012)

Pelo presente instrumento, eu, _____, CPF nº _____, Carteira de Identidade nº _____, expedida pelo _____, em _____, lotado (a) no(a) _____, neste hospital, na qualidade de USUÁRIO (A) da rede de computadores ou CUSTODIANTE de informações do Hospital das Forças Armadas (HFA), DECLARO TER CONHECIMENTO da Política de Segurança da Informação e Comunicações (PoSIC) do HFA e me comprometo a guardar o sigilo necessário, nos termos da Lei 12.527, de 18 de novembro de 2011, e a:

a) tratar as informações classificadas em qualquer grau de sigilo ou os materiais de acesso restrito que me forem fornecidos pelo Hospital das Forças Armadas ou outro órgão que este Hospital tiver relacionamento, e preservar o seu sigilo, de acordo com a legislação vigente;

b) preservar o conteúdo das informações classificadas em qualquer grau de sigilo, ou dos materiais de acesso restrito, sem divulgá-los a terceiros;

c) manter a confidencialidade das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

d) utilizar as credenciais de acesso (login e senha) e os recursos computacionais, em conformidade com a PoSIC do HFA e procedimentos estabelecidos em normas específicas do órgão;

e) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, observar a confidencialidade das informações sigilosas acessadas;

f) responder perante a Justiça, no âmbito, administrativo, penal e civil sobre o uso indevido dos recursos de tecnologia das informações disponibilizadas pelo HFA. Estou ciente de meu compromisso individual no HFA e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto no presente Termo e na legislação vigente.

Brasília-DF, ____ de _____ de _____.

_____
Assinatura (Usuário)

(NUP 60550.008431/2019-38)