MINISTÉRIO DA DEFESA

PORTARIA NORMATIVA Nº 1.688/MD, DE 5 DE AGOSTO DE 2015

Aprova a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa e dá outras providências.

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe são conferidas pelos incisos I e II do parágrafo único do art. 87 da Constituição, tendo em vista o disposto no Decreto nº 3.505, de 13 de junho de 2000; nos incisos XV e XVII do art. 27; nos incisos II, III, IV e V do art. 31 do Anexo I do Decreto nº 7.974, de 1º de abril de 2013, e considerando o que consta do Processo 60586.001035/2012-04, resolve:

Art. 1º Aprovar, nos termos do Anexo a esta Portaria Normativa, a Política de Segurança da Informação e Comunicações (PoSIC), com a finalidade de fornecer diretrizes, critérios e suporte administrativo para a implementação da Segurança da Informação e Comunicações (SIC) no âmbito da Administração Central do Ministério da Defesa (ACMD).

Parágrafo único. A PoSIC se aplica às atividades dos usuários da ACMD e os obriga ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 2º O Centro Gestor e Operacional do Sistema de Proteção da Amazônia (Censipam), o Hospital das Forças Armadas (HFA) e o Centro de Catalogação das Forças Armadas (Cecafa), devido às suas especificidades, serão regidos por Política de Segurança de Informação e Comunicações própria, alinhada, no que couber, à PoSIC anexa a esta Portaria Normativa, a qual deve ser submetida, no prazo de noventa dias, à avaliação e à aprovação do Comitê de Segurança da Informação e Comunicações (CSIC).

Art. 3º A íntegra da PoSIC da ACMD será disponibilizada no endereço eletrônico www.defesa.gov.br, no Portal do Ministério da Defesa (MD) e também em sua Intranet.

Art. 4º Esta Portaria Normativa entra em vigor na data de sua publicação.

Art. 5º Fica revogada a Portaria Normativa nº 1.530/MD, de 14 de maio de 2013.

JAQUES WAGNER

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
DA ADMINISTRAÇÃO CENTRAL DO MINISTÉRIO DA DEFESA

1. ESCOPO

1.1. A Política de Segurança da Informação e Comunicações (PoSIC) tem por objetivo instituir e implementar diretrizes estratégicas, responsabilidades e competências que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA) das informações no âmbito da Administração Central do Ministério da Defesa (ACMD).

1.2. A PoSIC trata do uso e do compartilhamento de dados, informações e documentos no âmbito da ACMD, em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

1.3. Integram também a PoSIC as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

2. CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos desta Política entende-se por:

a) Assinatura digital: conjunto de dados criptografados, associados a determinado documento/arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;
b) Ativo de informação: patrimônio composto por dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;
c) 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 ACMD;
d) Computação em nuvem: modelo computacional que permite acesso, por demanda e independente da localização, a conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;
e) Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
f) Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, ou seja: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;
g) Dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, dentre eles: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;
h) Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;
i) Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses

das partes envolvidas, a reputação e a marca daorganização, assim como seus processos e seu valor agregado. 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;

j) Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à Tecnologia da Informação e Comunicações (TIC);
k) Gestão de Riscos em Segurança da Informação e Comunicações: conjunto de processos que permite 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;
l) Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da ACMD;
m) Inventário e Mapeamento de Ativos de Informação: processo interativo e evolutivo, composto por três etapas:
    i. 1ª Etapa: A identificação e classificação de ativos de informação;
    ii. 2ª Etapa: Identificação de potenciais ameaças e vulnerabilidades; e
    iii. 3ª Etapa: Avaliação de riscos.
n) Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
o) Recurso Criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;
p) Segurança da Informação e Comunicações (SIC): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
q) Termo de Compromisso Individual (TCI): documento formal, a ser assinado pelos usuários da ACMD, por meio do qual é estabelecido vínculo de comprometimento pessoal com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
r) Termo de Confidencialidade (TC): documento formal, a ser assinado por prestadores de serviço da ACMD, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;
s) Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;
t) Usuários: servidores, militares, terceirizados, colaboradores, consultores, auditores, estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de informação da ACMD, formalizada por meio da assinatura do TCI.

3. REFERÊNCIAS

3.1. A PoSIC da ACMD foi elaborada com base nas seguintes referências legais e normativas:

- Lei nº 8.112, de 11 de dezembro de 1990;
- Lei nº 9.983, de 14 de julho de 2000;
- Lei nº 12.527, de 18 de novembro de 2011;
- Decreto nº 3.505, de 13 de junho de 2000;
- Decreto nº 5.482, de 30 de junho de 2005;
- Decreto nº 7.724, de 16 de maio de 2012;

- Decreto nº 7.845, de 14 de novembro de 2012.
- Decreto nº 7.974, de 1º de abril de 2013;
- Decreto nº 8.135, de 4 de novembro de 2013;
- Instrução Normativa GSI nº 1, de 13 de junho de 2008, e respectivas normas complementares;
- Instrução Normativa nº 04 SLTI/MP, de 11 de setembro de 2014;
- Portaria Normativa nº 142/MD, de 25 de janeiro de 2008;
- Portaria Normativa nº 1.704/MD, de 26 de junho de 2012;
- Portaria Interministerial MP/MC/MD nº 141 de 2 maio de 2014;
- Norma ABNT NBR/ISO/IEC 27001/2006; e
- Norma ABNT NBR/ISO/IEC 27002/2007

4. PRINCÍPIOS

4.1. A PoSIC da ACMD orienta-se pelos seguintes princípios:

a) Disponibilidade: garante que a informação estará acessível e utilizável por pessoa física, sistema, órgão ou entidade, quando requisitada;
b) Integridade: garante que a informação não será modificada, gravada ou excluída sem autorização ou acidentalmente;
c) Confidencialidade: garante que a informação será acessada apenas por pessoa física, sistema, órgão ou entidade autorizada e credenciada;
d) Autenticidade: garante a identificação de pessoa física, sistema, órgão ou entidade que produziu, expediu, modificou ou excluiu a informação.

4.2. As ações de SIC, no âmbito da ACMD, são norteadas pelos seguintes princípios:

a) Criticidade: define a importância da informação para a continuidade do negócio da organização;
b) Celeridade: garante respostas rápidas a incidentes e falhas de segurança;
c) Clareza: as regras e a documentação sobre segurança da informação e comunicações devem ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;
d) Ética: preserva o direito do servidor, militar, colaborador, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação e comunicações;
e) Legalidade: devem ser levadas em consideração as leis, as normas e as políticas organizacionais administrativas, técnicas e operacionais vigentes;
f) Responsabilidade: os usuários são responsáveis pelo cumprimento desta PoSIC e devem respeitar a legislação e normas pertinentes à Segurança da Informação e Comunicações vigentes.

4.3. São observados, ainda, sem prejuízo dos demais, os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a APF.

5. DIRETRIZES GERAIS

5.1. Pressupostos básicos

5.1.1. O sucesso das ações nos assuntos de segurança da informação e comunicações está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

5.1.2. A informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.

5.2. Para cada uma das diretrizes constantes das Seções deste Capítulo devem ser elaboradas normas técnicas específicas, manuais e procedimentos.

5.3. Tratamento da Informação

5.3.1. Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade do MD e deve ser protegida segundo as diretrizes descritas nesta PoSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do órgão e preservar sua imagem.

5.3.2. É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo MD.

5.3.3. Os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos de negócio do MD.

5.3.4. 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.

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

5.3.6. As informações produzidas ou custodiadas pelo MD devem ser descartadas conforme o seu nível de classificação.

5.3.7. Deve ser disponibilizada uma solução de Gestão Eletrônica de Documentos (GED) com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa.

5.3.8. A manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor.

5.4. Tratamento de Incidentes de Rede

5.4.1. A área de Tecnologia da Informação (TI) do MD manterá 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.

5.5.Gestão de Risco

5.5.1. Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação e comunicações.

5.5.2. Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito da ACMD.

5.5.3. O processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade, conforme procedimentos definidos em norma específica sobre o tema.

5.6. Gestão de Continuidade

5.6.1. O MD deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

5.6.2. As informações de propriedade ou custodiadas pelo MD, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança, de forma a garantir a continuidade das atividades do órgão.

5.6.3. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

5.7. Auditoria e Conformidade

5.7.1. O MD deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o acompanhamento, o controle e a verificação de acessos aos sistemas corporativos e rede interna do MD.

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

5.7.3. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o MD.

5.7.4. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

5.7.5. Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade.

5.8.Controle de Acesso

5.8.1. O controle de acesso aos sistemas corporativos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico definidos em norma específica, em conformidade com as diretrizes desta PoSIC.

5.9. Uso de E-mail (Correio Eletrônico)

5.9.1. O uso de e-mail no âmbito da ACMD deve ser definido em norma específica, com controle do uso e cancelamento de acesso ao correio eletrônico.

5.10. Acesso à Internet

5.10.1. O acesso à rede mundial de computadores (Internet), no âmbito da ACMD, será regido por norma interna, em conformidade com as diretrizes desta PoSIC, orientações governamentais e legislações específicas em vigor.

5.11. Inventário e Mapeamento de Ativos de Informação

5.11.1. Nos aspectos relacionados à SIC, o processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios para a Gestão de SIC, Gestão de Riscos de SIC, Gestão

de Continuidade de Negócios, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de geração da base de dados sobre os ativos de informação.

5.11.2. O processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

5.12. Dispositivos Móveis

5.12.1. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da ACMD 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.

5.13. Computação em Nuvem

5.13.1. As ações de segurança da informação e comunicações para a implementação ou a contratação, no âmbito da ACMD, de tecnologias de computação em nuvem devem estar em conformidade com as orientações definidas em norma e legislações específicas em vigor.

5.14. Criptografia

5.14.1. A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico baseado em algoritmo de Estado, conforme procedimentos definidos em norma e legislações específicas em vigor.

5.15. Redes Sociais

5.15.1. O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades estabelecidas, visando ao uso seguro das redes sociais, conforme procedimentos definidos em normas e legislações específicas em vigor.

5.16. Contratação de Serviços

5.16.1. Nos editais de licitação e nos contratos de empresas prestadoras de serviços com a ACMD deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta PoSIC, bem como ser exigida da empresa contratada e do prestador a assinatura do Termo de Compromisso Individual e do Termo de Confidencialidade.

5.16.2. A empresa contratada também deverá demonstrar que possui mecanismos que assegurem a segurança das informações do MD por ela acessadas direta ou indiretamente (acesso aos ativos que contêm informações) e cumprir o disposto nesta PoSIC quando aplicável.

5.16.3. Não poderá ser objeto de contratação a Gestão de Processos de Tecnologia da Informação ou a Gestão de Segurança da Informação.

5.16.4. O apoio técnico aos processos de planejamento e avaliação da qualidade das soluções de tecnologia da informação e comunicações poderá ser objeto de contratação, desde que sob supervisão exclusiva de servidores do MD.

5.16.5. Os termos e procedimentos para contratação de serviços terceirizados serão detalhados em norma complementar específica.

6. PENALIDADES

6.1. O usuário responderá pelo prejuízo que vier a ocasionar ao MD em decorrência do descumprimento de uma ou mais regras previstas nesta PoSIC.

6.2. A desobediência às regras estabelecidas implicará ao infrator as penalidades previstas em lei, nos âmbitos administrativo, civil, penal e militar.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1. Gestor de Segurança da Informação e Comunicações:

7.1.1. Planejar e coordenar a execução das ações de SIC;

7.1.2. Definir estratégias para a implementação desta PoSIC e normas complementares;

7.1.3. Supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de SIC;

7.1.4. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;

7.1.5. Encaminhar os fatos apurados, decorrentes de quebras de segurança, para a aplicação das penalidades previstas;

7.1.6. Gerenciar a análise de risco;

7.1.7. 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 normativos internos específicos;

7.1.8. Providenciar a divulgação interna e permanente desta PoSIC.

7.2. Comitê de Segurança da Informação e Comunicações:

7.2.1. Atualizar a Política de Segurança da Informação e Comunicações;

7.2.2. Propor grupos de trabalho para tratar de temas e sugerir soluções específicas sobre a segurança da informação e comunicações;

7.2.3. Propor, analisar e aprovar normas relativas à segurança da informação e comunicações, em conformidade com as legislações vigentes sobre o tema;

7.2.4. Propor um programa de Gestão de Continuidade de Negócios, com vistas a minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do MD, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

7.3. Área de Tecnologia da Informação:

7.3.1. Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC relacionadas com as diretrizes desta PoSIC;

7.3.2. Elaborar, implementar e atualizar normas internas específicas em conformidade com esta PoSIC e demais diretrizes do Governo;

7.3.3. Criar e manter a ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores;

7.3.4. Manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais do MD;

7.3.5. Manter uma unidade de Segurança da Informação e Comunicações com a responsabilidade de apoiar o Gestor de Segurança da Informação e Comunicações no cumprimento de suas atribuições;

7.4. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:

7.4.1. Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

7.4.2. Promover a recuperação de sistemas;

7.4.3. Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de rede por meio de verificações de conformidade;

7.4.4. Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

7.4.5. Analisar ataques e intrusões na rede do MD;

7.4.6. Executar as ações necessárias para tratar quebras de segurança;

7.4.7. Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

7.4.8. Cooperar com outras equipes de Tratamento e Resposta a Incidentes.

7.5. Setor de Recursos Humanos:

7.5.1. Comunicar ao Gestor de SIC, por meio de memorando, a ausência ou o desligamento de pessoal do MD;

7.5.2. Definir, nas descrições de cargos e funções, as responsabilidades pela manutenção das ações de SIC, bem como colher a assinatura do Termo de Compromisso Individual e do Termo de Confidencialidade que envolvam o manuseio dos ativos de informação;

7.5.3. Promover a ambientação de todo o pessoal, civil e militar, nomeado e/ou designado para a ACMD, por meio de treinamento e capacitação, com vistas a permitir acesso aos sistemas corporativos e às informações nos níveis físico e lógico, definidos em norma específica, em conformidade com as diretrizes desta PoSIC.

7.6. Usuário:

7.6.1. Acessar a rede de dados do MD somente após tomar ciência das normas de SIC e assinar o TCI;

7.6.2. Tratar a informação digital como patrimônio do MD e como recurso que deva ter seu sigilo preservado;

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

7.6.4. Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

7.6.5. Não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança (CredSeg) ou cujo teor não tenha autorização ou necessidade de conhecer;

7.6.6. Não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;

7.6.7. No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;

7.6.8. Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional do MD por terceiros;

7.6.9. Responder, perante o MD, por acessos, tentativas de acesso ou uso indevido da informação digital, realizados com a sua identificação ou autenticação;

7.6.10. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

7.6.11. Não transferir qualquer tipo de arquivo que pertença ao MD para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

7.6.12. Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional do MD;

7.6.13. Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional do MD pode ser auditada;

7.6.14. Estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da ACMD deve obedecer a esse preceito;

7.6.15. Ao assinar o TCI, o usuário declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PoSIC.

7.7. Custodiante da Informação:

7.7.1. Cumprir e zelar pela observância integral das diretrizes desta PoSIC e demais normas e procedimentos decorrentes;

7.7.2. Zelar pela disponibilidade, integridade, confidencialidade e autenticidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições

estabelecidas nesta PoSIC e demais normas e procedimentos decorrentes, mediante assinatura do TCI;

7.7.3. Participar de capacitação e treinamento em segurança da informação e comunicações, quando convocado;

7.7.4. Utilizar os recursos que lhe foram concedidos somente para o fim a que se destinam;

7.7.5. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

7.7.6. Preservar a classificação do grau de sigilo a documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções;

7.7.7. Comunicar prontamente ao seu Chefe imediato e ao Gestor de Segurança da Informação e Comunicações qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e recursos em qualquer suporte sob sua custódia.

8. DIVULGAÇÃO

8.1. A PoSIC e suas atualizações, após publicação, deverão ser divulgadas amplamente aos usuários da ACMD e disponibilizadas no Portal do MD e também em sua Intranet.

9. ATUALIZAÇÃO

9.1. A atualização desta PoSIC e instrumentos normativos adicionais obedecerão aos seguintes critérios:

9.1.1. Política - Nível de Aprovação: Ministro de Estado da Defesa. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de três anos;

9.1.2. Normas - Nível de Aprovação: Comitê de Segurança da Informação e Comunicações. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de dois anos;

9.1.3. Procedimentos - Nível de Aprovação: Responsável pela área envolvida. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de um ano.

10. ANEXOS

10.1. Termo de Compromisso Individual.

10.2. Termo de Confidencialidade.

ANEXO II

MINISTÉRIO DA DEFESA

S E C R E TA R I A - G E R A L

SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE COMPROMISSO INDIVIDUAL

Pelo presente instrumento, eu,_____, CPF nº _____, Carteira de Identidade nº_____, expedida pelo _____ em_____, lotado(a) no(a)_____ _____, neste Ministério, na qualidade de USUÁRIO (A) da rede de computadores ou CUSTODIANTE de informações da Administração Central do Ministério da Defesa (ACMD), DECLARO TER CONHECIMENTO da Política de Segurança da Informação e Comunicações (PoSIC) da ACMD, segundo a qual, sem restar qualquer dúvida de minha parte, devo:

a) tratar a informação como patrimônio do Ministério da Defesa (MD);

b) utilizar as informações e os recursos, em qualquer suporte sob minha custódia, exclusivamente no interesse do serviço do MD;

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 da ACMD 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 o MD pelo uso indevido das minhas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil.

Estou ciente de meu compromisso individual no Ministério da Defesa 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)

_____
Assinatura
(Representante da Unidade de Segurança da Informação e Comunicações)

ANEXO III

MINISTÉRIO DA DEFESA

S E C R E TA R I A - G E R A L

SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE CONFIDENCIALIDADE

A _____, inscrita no CNPJ sob o nº _____, sediada _____, por intermédio de seu representante legal, Sr. (a.)_____, portador(a) da Cédula de Identidade nº _____, expedida pelo (a)_____ e CPF nº _____, DECLARA que, para fins da execução do contrato no _____, comprometemo-nos a manter em sigilo, ou seja, não revelar ou divulgar as informações confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços nas instalações do Ministério da Defesa, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a eles se referem e ainda respeitar as normas de segurança vigentes.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o Ministério da Defesa de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, danos, perdas, custas e despesas que porventura venha a sofrer como resultado da violação do disposto neste instrumento.

_____
Local e Data

_____
Nome, Cargo e Assinatura
(Representante da Licitante)