



DIÁRIO OFICIAL DA UNIÃO



Publicado em: 11/01/2019 | Edição: 8 | Seção: 1 | Página: 11
Orgão: Ministério da Defesa/Gabinete do Ministro

PORTARIA NORMATIVA Nº 2/GM-MD, DE 3 DE JANEIRO DE 2019

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 da atribuição que lhe confere o Decreto, de 1º de janeiro de 2019, os incisos I e II do parágrafo único do art. 87 da Constituição, tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, e nos incisos X e XII do art. 32 e no art. 37 do Anexo I do Decreto nº 9.570, de 20 de novembro de 2018, e considerando o que consta do Processo nº 60586.00503/2018-19, resolve:

Art. 1º Fica aprovada, nos termos do Anexo I desta Portaria Normativa, a Política de Segurança da Informação e Comunicações, com o objetivo de estabelecer diretrizes, critérios e suporte administrativo para a implementação da Segurança da Informação e Comunicações no âmbito da administração central do Ministério da Defesa.

Parágrafo único. A Política de Segurança da Informação e Comunicações se aplica às atividades dos usuários da administração central do Ministério da Defesa 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, o Hospital das Forças Armadas e o Centro de Apoio a Sistemas Logísticos de Defesa, devido às suas especificidades, serão regidos por Políticas de Segurança da Informação e Comunicações próprias, alinhadas, no que couber, à Política de Segurança da Informação e Comunicações da administração central do Ministério da Defesa.

Art. 3º As Políticas de Segurança da Informação e Comunicações do Centro Gestor e Operacional do Sistema de Proteção da Amazônia, do Hospital das Forças Armadas e do Centro de Apoio a Sistemas Logísticos de Defesa deverão ser submetidas à avaliação e à aprovação do Comitê de Segurança da Informação e Comunicações da administração central do Ministério da Defesa, antes de serem aprovadas por seus respectivos órgãos.

Art. 4º A íntegra da Política de Segurança da Informação e Comunicações da administração central do Ministério da Defesa será disponibilizada no Portal do Ministério da Defesa e também em sua Intranet.

Art. 5º Fica revogada a Portaria Normativa nº 1.688/MD, de 5 de agosto de 2015.

Art. 6º Esta Portaria Normativa entra em vigor na data de sua publicação.

FERNANDO AZEVEDO E SILVA

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 estabelecer diretrizes, critérios e suporte administrativo para a implementação da Segurança da Informação e Comunicações (SIC) visando a garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações no âmbito da administração central do Ministério da Defesa.

1.2. A POSIC trata do uso e do compartilhamento de dados, informações e documentos no âmbito da administração central do Ministério da Defesa, 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 de Segurança entende-se por:

a. Assinatura digital: conjunto de dados criptografados, associados a determinado documento ou 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. Banco de Dados (ou Base de Dados): é um sistema de armazenamento de dados, ou seja, um conjunto de registros que tem como objetivo organizar e guardar as informações;

d. Cópia de Segurança (Backup): copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade. Essencial para dados importantes;

e. 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 central do Ministério da Defesa;

f. 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;

g. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

h. 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;

i. 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;

j. 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;

k. 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 da organização, 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;

l. 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);

m. 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;

n. Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da administração central do Ministério da Defesa;

o. Inventário e Mapeamento de Ativos de Informação: processo iterativo e evolutivo, composto por três etapas:

1. A identificação e classificação de ativos de informação;
2. Identificação de potenciais ameaças e vulnerabilidades; e
3. Avaliação de riscos.

p. 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;

q. Recurso Criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

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

s. Termo de Responsabilidade (TR): termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso;

t. Termo de Confidencialidade (TC): documento formal, a ser assinado por prestadores de serviço da administração central do Ministério da Defesa, por meio do qual se comprometem a manter sigilo em relação às informações consideradas confidenciais e respeitar as normas de segurança vigentes;

u. Tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

v. Trilhas de Auditoria: são rotinas específicas programadas nos sistemas para fornecerem informações de interesse da auditoria. São entendidas como o conjunto cronológico de registros (logs) que proporcionam evidências do funcionamento do sistema. Esses registros podem ser utilizados para reconstruir, rever/revisar e examinar transações desde a entrada de dados até a saída dos resultados finais, bem como para avaliar/rastrear o uso do sistema, detectando e identificando usuários não autorizados; e

w.Usuários: servidores, militares, terceirizados, consultores, auditores, estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação da administração central do Ministério da Defesa, formalizada por meio da assinatura do Termo de Responsabilidade.

3. REFERÊNCIAS

3.1. A POSIC da administração central do Ministério da Defesa foi elaborada com base nas seguintes referências legais e normativas:

- Lei nº 7.232, de 29 de outubro de 1984;
- 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;
- Lei nº 12.737, de 30 de novembro de 2012;
- Lei nº 12.965, de 23 de abril de 2014;
- 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 8.978, de 1º de fevereiro de 2017;
- 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 MP/SLTI nº 4, de 11 de setembro de 2014;
- Portaria Normativa nº 564/MD, de 12 de março de 2014;
- Portaria 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;
- Norma ABNT NBR/ISO/IEC 27002/2007; e
- Código Penal Brasileiro (Decreto-Lei nº 2.848, de 7 de dezembro de 1940).

4. PRINCÍPIOS

4.1. A POSIC da administração central do Ministério da Defesa 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; e
- 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 administração central do Ministério da Defesa, 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; e
- 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 Administração Pública Federal.

5. DIRETRIZES GERAIS

5.1. Esta POSIC tem como principal diretriz a preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação da administração central do Ministério da Defesa.

5.2. Pressupostos básicos

5.2.1. 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.

5.2.2. 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.

5.2.3. A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, disponibilidade, conformidade e confidencialidade.

5.2.4. Todos os membros, servidores e estagiários da administração central do Ministério da Defesa e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional da administração central do Ministério da Defesa e sejam usuários dos ativos sigilosos, devem assinar o Termo de Responsabilidade quanto ao sigilo dos dados, informações e conhecimentos da administração central do Ministério da Defesa.

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

5.4. Tratamento da Informação

5.4.1. Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade da administração central do Ministério da Defesa 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.

5.4.2. 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 pela administração central do Ministério da Defesa.

5.4.3. Os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos de negócio da administração central do Ministério da Defesa.

5.4.4. 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.

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

5.4.6. As informações produzidas ou custodiadas pela administração central do Ministério da Defesa devem ser descartadas conforme o seu nível de classificação.

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

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

5.4.9. A destruição de dados sigilosos deve ser feita por método que sobrescreva as informações armazenadas. Se não estiver ao alcance do órgão a destruição lógica, deverá ser providenciada a destruição física por incineração dos dispositivos de armazenamento.

5.5. Tratamento de Incidentes de Rede

5.5.1. O Departamento de Tecnologia da Informação e Comunicação manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

5.5.2. Sua criação, sua estrutura e seu modelo de implementação serão definidas em Portaria Normativa que deverá estar em conformidade com as diretrizes desta POSIC.

5.6. Gestão de Risco

5.6.1. 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.

5.6.2. 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 administração central do Ministério da Defesa.

5.6.3. 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.

5.7. Gestão de Continuidade

5.7.1. A administração central do Ministério da Defesa 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.

5.7.2. As informações de propriedade ou custodiadas pela administração central do Ministério da Defesa, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança atualizada e guardada em local remoto, de forma a garantir a continuidade das atividades do órgão.

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

5.8. Auditoria e Conformidade

5.8.1. O Ministério da Defesa 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 da administração central do Ministério da Defesa.

5.8.2. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC aplicadas na administração central do Ministério da Defesa com esta POSIC, bem como com a legislação específica em vigor.

5.8.3. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a administração central do Ministério da Defesa.

5.8.4. 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.

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

5.8.6. Os procedimentos e as metodologias utilizados na auditoria e conformidade no âmbito da administração central do Ministério da Defesa serão definidos em norma específica, em conformidade com as diretrizes desta POSIC e demais legislações em vigor.

5.9. Controle de Acesso

5.9.1. 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 e serão definidos em norma específica, em conformidade com as diretrizes desta POSIC.

5.10. Uso de e-mail (correio eletrônico)

5.10.1. O uso de e-mail no âmbito da administração central do Ministério da Defesa deve ser definido em norma específica, em conformidade com as diretrizes desta POSIC, e deve tratar, dentre outras coisas, do controle de acesso.

5.11. Acesso à Internet

5.11.1. O acesso à rede mundial de computadores (Internet), no âmbito da administração central do Ministério da Defesa, deve ser definido em norma específica, em conformidade com as diretrizes desta POSIC, orientações governamentais e legislações específicas em vigor.

5.12. Inventário e Mapeamento de Ativos de Informação

5.12.1. 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.

5.12.2. 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, conseqüentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

5.13. Dispositivos Móveis

5.13.1. O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da administração central do Ministério da Defesa deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário e ser definido em norma específica, em conformidade com as diretrizes desta POSIC.

5.14. Computação em Nuvem

5.14.1. A implementação ou contratação de computação em nuvem no âmbito da administração central do Ministério da Defesa deve ser definida em norma específica, em conformidade com as diretrizes desta POSIC e com as demais legislações vigentes sobre o tema.

5.15. Criptografia

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

5.15.2. Qualquer sistema utilizado na administração central do Ministério da Defesa e que contenham tabelas com senhas, deverão ter estas tabelas armazenadas criptografadas;

5.16. Redes Sociais

5.16.1. O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades, definidas em norma complementar, em conformidade com as diretrizes desta POSIC.

5.17. Contratação de Serviços

5.17.1. Nos editais de licitação e nos contratos de empresas prestadoras de serviços com a administração central do Ministério da Defesa deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta POSIC, bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade e do Termo de Confidencialidade.

5.17.2. A empresa contratada também deverá demonstrar que possui mecanismos que assegurem a segurança das informações da administração central do Ministério da Defesa por ela acessadas direta ou indiretamente (acesso aos ativos que contêm informações) e cumprir o disposto nesta POSIC quando aplicável.

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

5.17.4. 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 da administração central do Ministério da Defesa.

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

6. COMPETÊNCIAS

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

6.1.1. Atualizar a POSIC;

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

6.1.3. Tratar dos assuntos de Segurança da Informação no âmbito da administração central do Ministério da Defesa e assessorar diretamente o Gestor de Segurança da Informação e Comunicações;

6.2. Ao Departamento de Tecnologia da Informação e Comunicação compete:

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

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

6.2.3. 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 da administração central do Ministério da Defesa;

6.2.4. 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. À Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais compete:

6.3.1. Coordenar as atividades de tratamento e resposta a incidentes de segurança;

6.3.2. Promover a recuperação de sistemas;

6.3.3. 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;

6.3.4. 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;

6.3.5. Receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores da administração central do Ministério da Defesa;

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

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

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

6.4. Setor de Recursos Humanos:

6.4.1. Comunicar mensalmente ao Gestor de SIC, por meio de memorando, o ingresso, a alteração de lotação ou localização, bem como o desligamento de pessoal civil e militar, inclusive postos terceirizados, no âmbito da administração central do Ministério da Defesa;

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

6.4.3. Mediante conteúdos e objetivos específicos propostos pela(s) área(s) de TIC da administração central do Ministério da Defesa, promover a inserção e a atualização, gradativa e periódica, do pessoal civil e militar, inclusive postos terceirizados, com vistas a permitir a utilização de sistemas corporativos e acesso a informações nos níveis físico e lógico, conforme norma específica, em conformidade com as diretrizes desta POSIC.

7. ATRIBUIÇÕES

7.1. O Gestor de Segurança da Informação e Comunicações possui as seguintes atribuições:

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

7.1.2. Definir estratégias para a implementação desta POSIC e suas 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 SIC estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativos internos específicos; e

7.1.8. Providenciar a divulgação interna e permanente desta POSIC e de suas normas complementares.

8. RESPONSABILIDADES

8.1. Usuário:

8.1.1. Acessar a rede de dados da administração central do Ministério da Defesa somente após tomar ciência das normas de SIC e assinar o Termo de Responsabilidade;

8.1.2. Tratar a informação digital como patrimônio do Ministério da Defesa e como recurso que deva ter seu sigilo preservado;

8.1.3. Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso do Ministério da Defesa exclusivamente para o interesse do serviço;

8.1.4. 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;

8.1.5. 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;

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

8.1.7. 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;

8.1.8. Não compartilhar, transferir, divulgar ou permitir o conhecimento de credenciais de acesso (senhas) utilizadas no ambiente computacional da administração central do Ministério da Defesa por terceiros;

8.1.9. Responder perante o Ministério da Defesa pelo uso indevido das suas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil;

8.1.10. 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;

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

8.1.12. Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço não são permitidos na rede computacional da administração central do Ministério da Defesa;

8.1.13. Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional da administração central do Ministério da Defesa pode ser auditada;

8.1.14. 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 administração central do Ministério da Defesa deve obedecer a esse preceito;

8.1.15. Ao assinar o Termo de Responsabilidade, o usuário declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta POSIC; e

8.1.16. Utilizar as credenciais de acesso (login e senha) e os recursos computacionais, em conformidade com a POSIC da administração central do Ministério da Defesa e procedimentos estabelecidos em normas específicas do órgão.

8.2. Custodiante da Informação:

8.2.1. Cumprir e zelar pela observância integral das diretrizes desta POSIC e demais normas e procedimentos decorrentes;

8.2.2. 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 Termo de Responsabilidade;

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

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

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

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

8.2.7. 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.

9. DIVULGAÇÃO

9.1. A POSIC e suas atualizações, após publicação, deverão ser divulgadas amplamente aos usuários da administração central do Ministério da Defesa e disponibilizadas no Portal do Ministério da Defesa e também em sua Intranet.

10. ATUALIZAÇÃO

10.1. A atualização desta POSIC e instrumentos normativos adicionais obedecerão aos seguintes critérios:

10.1.1. 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;

10.1.2. 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;

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

11. PENALIDADES

11.1. O usuário responderá pelo prejuízo que vier a ocasionar ao Ministério da Defesa em decorrência do descumprimento de uma ou mais regras previstas nesta POSIC.

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

ANEXO II

MINISTÉRIO DA DEFESA

SECRETARIA-GERAL

SECRETARIA DE ORÇAMENTO E ORGANIZAÇÃO INSTITUCIONAL

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE RESPONSABILIDADE

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 (administração central do Ministério da Defesa), declaro ter conhecimento da Política de Segurança da Informação e Comunicações da administração central do Ministério da Defesa, segundo a qual, sem restar qualquer dúvida de minha parte, devo cumprir todas as suas diretrizes e orientações.

Estou ciente de meu compromisso no Ministério da Defesa e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto na POSIC da administração central do Ministério da Defesa e na legislação vigente.

Brasília - DF, ____ de _____ de _____

Assinatura

(Usuário)

ANEXO III

MINISTÉRIO DA DEFESA

SECRETARIA-GERAL

SECRETARIA DE ORÇAMENTO E ORGANIZAÇÃO INSTITUCIONAL

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

TERMO DE CONFIDENCIALIDADE

A _____, inscrita no CNPJ sob o nº _____, sediada _____, por intermédio de seu representante legal, o 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)

Este conteúdo não substitui o publicado na versão certificada (pdf).

