DIÁRIO OFICIAL DA UNIÃO

Publicado em: 28/11/2022 | Edição: 223 | Seção: 1 | Página: 12

Órgão: Ministério da Defesa/Gabinete do Ministro

PORTARIA GM-MD Nº 5.659, DE 18 DE NOVEMBRO DE 2022

Aprova a Política de Segurança da Informação da administração central do Ministério da Defesa - POSIN-MD.

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, tendo em vista o disposto no art. 15, inciso II, do Decreto nº 9.637, de 26 de dezembro de 2018, na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e de acordo com o que consta do Processo Administrativo nº 60220.000206/2022-91, resolve:

Art. 1º Esta Portaria aprova a Política de Segurança da Informação da administração central do Ministério da Defesa - POSIN-MD, na forma do Anexo.

Parágrafo único. A POSIN-MD tem o objetivo de estabelecer diretrizes, responsabilidades e competências para a gestão da segurança da informação no âmbito da administração central do Ministério da Defesa.

Art. 2º A Escola Superior de Guerra - ESG, a Escola Superior de Defesa - ESD e o Hospital das Forças Armadas - HFA, devido às suas especificidades, serão regidos por políticas de segurança da informação editadas pelos respectivos Comandantes, observadas, no que couber, as disposições da POSIN-MD.

Parágrafo único. As propostas de política de segurança da informação de que tratam o caput deverão ser previamente submetidas à avaliação e à aprovação do Comitê de Segurança da Informação da administração central do Ministério da Defesa - CSIN-MD, antes de serem formalizadas no âmbito da ESG, da ESD e do HFA, observado o disposto no art. 3º, inciso VI, da Portaria GM-MD nº 3.247, de 8 de junho de 2022.

Art. 3º A íntegra da POSIN-MD será disponibilizada no sítio eletrônico do Ministério da Defesa e na sua intranet.

Art. 4º Fica revogada a Portaria Normativa nº 2/GM-MD, de 3 de janeiro de 2019, publicada no Diário Oficial da União nº 8, Seção 1, páginas 11 a 13, de 11 de janeiro de 2019.

Art. 5º Esta Portaria entra em vigor em 1º de dezembro de 2022.

PAULO SÉRGIO NOGUEIRA DE OLIVEIRA

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DA ADMINISTRAÇÃO CENTRAL DO MINISTÉRIO DA DEFESA - POSIN-MD

1. ESCOPO

1.1 A Política de Segurança da Informação da administração central do Ministério da Defesa - POSIN-MD tem por objetivo estabelecer diretrizes, responsabilidades e competências para a gestão da Segurança da Informação - SI visando a garantia da disponibilidade, da integridade, da confidencialidade e da autenticidade das informações no âmbito da administração central do Ministério da Defesa - ACMD.

1.2 A SI abrange a segurança cibernética, a defesa cibernética, a segurança física, a proteção dos dados organizacionais e as ações destinadas a assegurar a integridade, disponibilidade, autenticidade e confidencialidade da informação.

1.3 A POSIN-MD orienta o tratamento da informação no âmbito da ACMD, em todo o seu ciclo de vida (criação, coleta, manuseio, divulgação, armazenamento, retenção, processamento, compartilhamento e eliminação), considerando a privacidade e a segurança desde a concepção da informação, visando à continuidade, em especial, das atividades críticas, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de SI.

2. CONCEITOS E DEFINIÇÕES

2.1 Para os efeitos da POSIN-MD serão considerados os conceitos e definições constantes da Portaria GSI/PR nº 93, de 18 de outubro de 2021, que aprova o Glossário de Segurança da Informação, e suas atualizações, em especial:

a) atividade crítica: atividade que deve ser executada visando garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

b) ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

c) auditoria: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;

d) autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

e) confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

f) controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

g) defesa cibernética: ações realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente;

h) disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

i) gestão de continuidade de negócios em segurança da informação: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

j) integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

k) segurança cibernética: ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis; e

l) tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

3. PRINCÍPIOS

3.1 A POSIN-MD é orientada pelos princípios estabelecidos na Política Nacional de Segurança da Informação e pelos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal.

4. DIRETRIZES GERAIS

4.1 Pressupostos básicos:

4.1.1. 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.

4.1.2. O sucesso das ações nos assuntos de SI 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.

4.1.3. O sigilo das informações é responsabilidade de todos que a elas tenham acesso.

4.1.4. Os integrantes da ACMD devem zelar pela segurança física e do ambiente de suas instalações, bem como pela segurança dos dados organizacionais sob sua responsabilidade.

4.1.5. As normas complementares à POSIN-MD serão de conteúdo geral e de atendimento obrigatório por todos os órgãos da ACMD.

4.1.6. Os órgãos da ACMD, ao disciplinar questões relativas à segurança da informação, deverão manter suas normas, processos e procedimentos atualizados de acordo com a POSIN-MD e com as suas normas complementares.

4.1.7. A POSIN-MD e suas atualizações, após publicação, deverão ser disponibilizadas no sítio eletrônico do Ministério da Defesa e na sua intranet, ressalvadas as hipóteses de restrição de acesso ou de sigilo previstas na legislação aplicável à matéria.

4.2. Gestão de ativos

4.2.1. Nos aspectos relacionados à SI, o mapeamento de ativos de informação e o correspondente inventário devem produzir subsídios para a gestão de incidentes de Segurança da Informação, de riscos e de continuidade, bem como para os procedimentos de avaliação da conformidade, de melhorias contínuas, de auditoria e, principalmente, de estruturação e de administração da base de dados sobre os ativos de informação.

4.3. Tratamento da informação

4.3.1. Toda informação tratada por usuário, no exercício de suas atividades, é considerada bem e propriedade da ACMD e deve ser protegida segundo as diretrizes descritas na POSIN-MD e demais regulamentações em vigor.

4.3.2. 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 pela ACMD.

4.3.3. Os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de reduzir ameaças e minimizar riscos às atividades e aos objetivos de negócio da ACMD.

4.3.4. No tratamento das informações deve-se respeitar a classificação segundo o grau de sigilo, a criticidade e a proteção de dados pessoais, conforme normas internas e legislação específica em vigor.

4.3.5. A manipulação e a eliminação de informações classificadas em qualquer grau de sigilo devem seguir as normas internas e a legislação em vigor.

4.3.6. Os responsáveis pelos ativos de informação devem manter registros e procedimentos que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso, em especial aos sistemas corporativos e às redes computacionais.

4.4. Segurança física e do ambiente

4.4.1. Os gestores de segurança física e do ambiente deverão estabelecer os perímetros de segurança, regras de controle de acesso e aspectos de monitoramento, bem como outras medidas visando à segurança física e do ambiente.

4.5. Gestão de incidentes de segurança da informação

4.5.1. A criação, a estrutura e o modelo de implementação da(s) Equipe(s) de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) serão definidos em conformidade com as diretrizes da POSIN-MD.

4.5.2. Os incidentes que afetem dados pessoais deverão ser imediatamente comunicados ao Encarregado pelo Tratamento de Dados Pessoais, que orientará as práticas a serem adotadas.

4.5.3. Os custodiantes da informação realizarão a gestão de incidentes envolvendo a segurança física e do ambiente.

4.5.4. Todas as unidades organizacionais zelarão pela gestão dos dados organizacionais sob sua responsabilidade.

4.6. Gestão de risco

4.6.1. Risco de segurança da informação está associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, devendo ser continuamente monitorado e tratado, conforme legislação em vigor.

4.7. Gestão de continuidade

4.7.1. A implementação do processo de gestão de continuidade de negócios em SI tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

4.7.2. O processo de gestão de continuidade de negócios em SI deve se basear em um plano de continuidade de negócios em SI, estruturado a partir da análise e avaliação dos riscos de SI identificados e da prioridade de recuperação dos processos de negócio.

4.7.3. O gestor de SI coordenará o processo de gestão de continuidade de negócios em SI.

4.8. Auditoria e conformidade

4.8.1. Os custodiantes de ativos da informação devem estabelecer procedimentos de auditoria, com objetivo de averiguar se estão de acordo com as legislações, normas e procedimentos relacionados à SI em sua área de competência.

4.8.2. A avaliação de conformidade nos aspectos de SI visa proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis.

4.8.3. O processo de avaliação de conformidade nos aspectos de SI deve ser composto pelo plano de verificação de conformidade e pelo relatório de avaliação de conformidade, que serão elaborados pelos custodiantes dos ativos de informação.

4.9. Controle de acesso

4.9.1. O controle de acesso aos ativos de informação e às áreas e instalações deve ser implantado nos níveis físico e lógico, conforme procedimentos estabelecidos pelas áreas competentes.

4.9.2. O controle de acesso aos ativos de informação deverá conter identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

4.10. Gestão do uso de recursos operacionais e de comunicações.

4.10.1. O uso de recursos operacionais e de comunicação deve seguir procedimentos estabelecidos pelas áreas competentes em conformidade com a POSIN-MD e observando, no mínimo, o seguinte:

a) o correio eletrônico institucional é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais;

b) o acesso à Internet provido pelo MD deve ter seu uso disciplinado para a restrita execução das atividades funcionais;

c) o uso de dispositivos móveis de armazenamento deve ser controlado com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário;

d) a implementação ou contratação de computação em nuvem deve ser precedida de procedimentos de conformidade com a legislação vigente;

e) as informações classificadas em qualquer grau de sigilo devem ser protegidas mediante o emprego de recurso criptográfico adequado;

f) as tabelas que armazenam senha de acesso e autenticação devem ser criptografadas; e

g) critérios, limitações e responsabilidades no uso institucional das mídias sociais, em conformidade com a legislação aplicável à matéria.

4.11. Contratação de serviços

4.11.1. Nos editais de licitação e nos contratos deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas da POSIN-MD, bem como ser exigida da empresa contratada e do prestador de serviços a assinatura do Termo de Responsabilidade (Apêndice I) e do Termo de

Confidencialidade (Apêndice II), quando aplicável.

4.11.2. A empresa contratada também deverá manter mecanismos que garantam a segurança das informações por ela acessadas direta ou indiretamente.

4.11.3. A gestão de processos de tecnologia da informação ou a gestão de SI não poderá ser objeto de contratação para execução de forma indireta.

4.12. Trabalho remoto

4.12.1. As normas que disciplinem o trabalho remoto devem estabelecer critérios técnicos e responsabilidades, observando-se as condicionantes de integridade documental e de segurança de dados e informações afetas à sua área de atuação, em conformidade com a legislação vigente.

5. RESPONSABILIDADES E COMPETÊNCIAS

5.1. Compete à alta administração do Ministério da Defesa a governança da segurança da informação, que será exercida por intermédio do Comitê de Governança do Ministério da Defesa - CG-MD, subsidiado pelo Comitê de Segurança da Informação - CSIN.

5.2. Ao Comitê de Segurança da Informação compete:

a) deliberar sobre assuntos relativos à Política Nacional de Segurança da Informação no âmbito da ACMD;

b) assessorar quanto à implementação das ações de SI;

c) constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SI, observadas as regras do Decreto nº 9.759, de 11 de abril de 2019;

d) participar da elaboração, propor alterações e deliberar sobre normas complementares a esta POSIN-MD, na forma de diretrizes específicas, a serem observadas por todos os órgãos da ACMD;

e) propor alterações da POSIN-MD; e

f) subsidiar o CG-MD no exercício da governança da SI no âmbito da ACMD.

5.3. Ao Gestor de Segurança da Informação compete:

a) assessorar a alta administração na implementação da POSIN-MD;

b) coordenar o Comitê de Segurança da Informação;

c) coordenar programa de educação e conscientização em segurança da informação, visando implementar uma mentalidade de segurança;

d) promover a divulgação da POSIN-MD e das diretrizes específicas complementares, editadas pelo CSIN, a todos os servidores, usuários e prestadores de serviços;

e) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;

f) propor recursos orçamentários e humanos necessários às ações de SI;

g) acompanhar os trabalhos da(s) equipe(s) de prevenção, tratamento e resposta a incidentes cibernéticos;

h) verificar os resultados dos trabalhos de auditoria sobre a gestão da SI;

i) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI; e

j) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI.

5.4. Aos órgãos integrantes da ACMD responsáveis por redes computacionais, compete:

a) planejar, coordenar, supervisionar, executar e controlar a execução das atividades de tecnologia da informação em conformidade com as diretrizes da POSIN-MD;

b) elaborar, implementar e atualizar seus processos de trabalho e procedimentos em conformidade com a POSIN-MD, suas normas complementares e demais diretrizes do Governo;

c) estabelecer e manter sua equipe de prevenção, tratamento e respostas a incidentes cibernéticos; e

d) comunicar ao Gestor de SI incidentes de segurança que tenham o potencial de comprometer o funcionamento e/ou a imagem do MD.

5.5. À(s) equipe(s) de prevenção, tratamento e resposta a incidentes cibernéticos compete:

a) coordenar as atividades de prevenção, tratamento e resposta a incidentes de segurança na rede computacional de sua responsabilidade;

b) promover a recuperação de dados, serviços e sistemas de Tecnologia da Informação; e

c) cooperar com outras equipes de prevenção, tratamento e resposta a incidentes cibernéticos.

5.6. Aos gestores de recursos humanos, compete:

a) manter os dados cadastrais atualizados e disponíveis para os sistemas de controle de acesso, de modo a permitir o bloqueio ou a alteração de acesso de pessoal militar e civil, inclusive terceirizados, estagiários e temporários;

b) definir, nas descrições de cargos e funções, as responsabilidades pela manutenção das ações de SI, bem como colher a assinatura do Termo de Responsabilidade e, quando envolver o manuseio dos ativos de informação sigilosos, do Termo de Confidencialidade; e

c) disponibilizar materiais de ambientação com conceitos básicos, visando a conscientização em SI.

5.7. Aos gestores de segurança física e do ambiente, compete:

a) disciplinar os procedimentos de segurança física e do ambiente de acordo com a POSIN e com as suas normas complementares, difundindo, aplicando e fiscalizando seu cumprimento; e

b) coordenar e executar a segurança do perímetro externo sob sua responsabilidade, conforme legislação em vigor.

5.8. Aos usuários e custodiantes da informação, compete:

a) tratar os ativos da informação como patrimônio do Ministério da Defesa;

b) cumprir e zelar pela observância integral das diretrizes da POSIN-MD e demais normas e procedimentos decorrentes;

c) acessar os ativos de informação somente após tomar ciência da POSIN-MD e assinar o Termo de Responsabilidade (Apêndice I), atestando ter pleno conhecimento e aceitar expressamente, sem reservas, os termos da POSIN-MD;

d) comunicar prontamente ao seu Chefe imediato, e este, ao Gestor de Segurança da Informação, qualquer incidente de que tenha conhecimento ou situações que comprometam a segurança dos ativos de informação;

e) utilizar os ativos de informação, os sistemas e produtos computacionais de propriedade ou direito de uso do MD exclusivamente para o interesse do serviço;

f) 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;

g) acessar ou tentar acessar informação somente em grau de sigilo compatível com a sua Credencial de Segurança (CredSeg) ou para a qual tenha autorização e necessidade de conhecer;

h) proteger os ativos de informação contra acesso, modificação, destruição ou divulgação não autorizada;

i) usar exclusivamente a identificação para acesso próprio, não permitindo nem compartilhando, transferindo ou divulgando o conhecimento de credenciais de acesso de terceiros no âmbito da ACMD;

j) 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, firmando termo de responsabilidade específico, conforme o caso;

k) não transferir qualquer ativo de informação que pertença ao MD para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante permissão da autoridade competente;

l) estar ciente de que toda informação produzida, armazenada, processada e transmitida no âmbito do MD pode ser auditada pelo setor competente;

m) somente utilizar dispositivos portáteis de computação particulares nos limites estabelecidos na POSIN-MD e nas normas relacionadas, sem prejuízo da responsabilização em caso de incidentes de segurança decorrentes desse uso; e

n) participar de capacitação e treinamento em SI, quando convocado.

6. ATUALIZAÇÃO

6.1. A POSIN-MD e suas normas e procedimentos complementares deverão ser atualizados sempre que se fizer necessário, não excedendo o período de quatro anos, observadas as disposições da Portaria GM-MD nº 3.247, de 2022.

7. PENALIDADES

7.1. A inobservância às regras estabelecidas na POSIN-MD implicará ao infrator as penalidades previstas em lei, nos âmbitos administrativo, civil, penal e militar.

APÊNDICE I

MINISTÉRIO DA DEFESA

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu, _____ CPF nº _____ 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, declaro ter conhecimento da Política de Segurança da Informação (POSIN-MD) 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 com o Ministério da Defesa e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto na POSIN-MD da administração central do Ministério da Defesa e na legislação vigente.

Brasília/DF, _____ de _____ de _____

_____

Assinatura

(Usuário ou custodiante da informação)

APÊNDICE II

MINISTÉRIO DA DEFESA

TERMO DE CONFIDENCIALIDADE

Pelo presente instrumento, eu, _____ CPF nº _____ lotado(a) no(a) _____ neste Ministério ou representante legal da empresa inscrita no CNPJ sob o nº _____ sediada em _____ para fins da execução do contrato nº _____ comprometo-me a manter em sigilo, ou seja, não revelar ou divulgar as informações sigilosas ou de caráter não público recebidas durante e após o exercício funcional ou prestação dos serviços nas instalações do Ministério da Defesa.

A violação dos termos deste instrumento resultará na aplicação das penalidades previstas em lei, nos âmbitos administrativo, civil, penal e militar.

Brasília/DF, _____ de _____ de _____

_____

Assinatura