DIÁRIO OFICIAL DA UNIÃO

Publicado em: 31/05/2021 | Edição: 101 | Seção: 1 | Página: 20

Órgão: Ministério da Agricultura, Pecuária e Abastecimento/Gabinete da Ministra

# PORTARIA MAPA Nº 136, DE 25 DE MAIO DE 2021

Aprova a Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - PoSIC/MAPA.

A MINISTRA DE ESTADO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO, no uso das atribuições que lhe confere o art. 87, parágrafo único, inciso II, da Constituição Federal, tendo em vista o disposto no inciso II do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018, no art. 9º, caput, parágrafo único e, art. 10, caput, parágrafo único, ambos da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e o que consta do Processo nº 21000.056426/2020-40, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - PoSIC/MAPA, na forma do Anexo desta Portaria.

Art. 2º Revogam-se:

I - a Portaria MAPA nº 147, de 10 de julho de 2015;

II - a Portaria MAPA nº 1.068, de 14 de junho de 2017; e

III - as Normas Complementares PoSIC/MAPA nºs 1 a 8, de 14 de junho de 2017.

Art. 3º Esta Portaria entra em vigor em 1º de julho de 2021.

**TEREZA CRISTINA CORREA DA COSTA DIAS**

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES DO MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO - POSIC/MAPA

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - PoSIC/MAPA tem como finalidade estabelecer objetivos, princípios, diretrizes gerais, competências, penalidades e política de atualização das ações de segurança da informação nas áreas de competência previstas no art. 1º do Anexo I ao Decreto nº 10.253, de 20 de fevereiro de 2020, de forma a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação do MAPA.

Art. 2º A PoSIC/MAPA abrange os órgãos de assistência direta e imediata ao Ministro de Estado da Agricultura, Pecuária e Abastecimento, os órgãos específicos singulares e os órgãos colegiados de que tratam os incisos I, II e III do art. 2º do Anexo I ao Decreto nº 10.253, de 2020, bem como os agentes públicos lotados no MAPA.

§ 1º Os contratos firmados pelo MAPA deverão conter cláusulas que determinem a observância desta PoSIC/MAPA e de seus atos normativos complementares por parte do contratado, bem como de seus dirigentes, prepostos, administradores, representantes e colaboradores.

§ 2º As entidades vinculadas de que trata o inciso IV do art. 2º do Anexo I ao Decreto nº 10.253, de 2020, deverão editar suas respectivas políticas de segurança da informação e comunicações.

Art. 3º A PoSIC/MAPA deverá ser complementada por atos normativos ulteriores, conforme as competências definidas neste Anexo.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 4º Para efeitos desta Portaria, considera-se:

I - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

II - ativo: qualquer coisa que tenha valor para a organização;

III - ativos de informação: os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

IV - 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;

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

VI - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VII - custodiante da informação: qualquer indivíduo ou estrutura de órgão ou entidade da APF, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

VIII - 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;

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

X - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XI - segurança orgânica: conjunto de medidas passivas com o objetivo de prevenir e até mesmo obstruir as ações que visem ao comprometimento ou à quebra de segurança de uma organização. Inclui os processos relacionados às áreas: de pessoal, de documentação, das comunicações, da tecnologia da informação, dos materiais e das instalações de uma organização, dentre outros;

XII - serviços: um meio de fornecer valor a clientes, facilitando a obtenção de resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XIII - sistema de proteção física: sistema composto por pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas, conforme gestão da segurança física e ambiental;

XIV - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XV - 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;

XVI - tratamento da informação classificada: conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo; e

XVII - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

Parágrafo único. A implementação da PoSIC/MAPA observará a Portaria MAPA nº 375, de 23 de novembro de 2020, que aprovou o Plano Estratégico do MAPA para o período 2020-2031.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 5º São princípios da PoSIC/MAPA:

I - dever de garantir o sigilo de informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da vida privada, da honra e da imagem das pessoas;

II - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

III - visão abrangente e sistêmica da segurança da informação;

IV - preservação do acervo histórico do MAPA; V - educação como alicerce fundamental para o fomento da cultura da segurança da informação;

VI - orientação à gestão de riscos e à gestão da segurança da Informação;

VII - prevenção e tratamento de incidentes de segurança da Informação;

VIII - articulação entre ações de segurança cibernética e de proteção de dados e ativos de informação;

IX - need to know (necessidade de conhecer) para o acesso a informações sigilosas, nos termos da legislação vigente;

X - consentimento do proprietário da informação sigilosa recebida de outros países, nos casos de acordos internacionais;

XI - integração e cooperação entre MAPA, sociedade, instituições de ensino e pesquisa, setor produtivo e órgãos e entidades da administração pública direta e indireta da União, Estados, Distrito Federal e Municípios; e

XII - alinhamento ao planejamento estratégico do MAPA.

CAPÍTULO IV

DOS OBJETIVOS

Art. 6º São objetivos da PoSIC/MAPA:

I - orientar as ações de segurança da informação para a realização das competências previstas no art. 1º do Anexo I ao Decreto nº 10.253, de 2020;

II - aprimorar continuamente o arcabouço legal e normativo do MAPA relacionado à segurança da informação;

III - fomentar a formação e a qualificação de recursos humanos do MAPA necessários à segurança da informação;

IV - fortalecer a cultura da segurança da informação no MAPA;

V - orientar ações relacionadas com:

a) a segurança de dados e informações custodiados pelo MAPA;

b) a segurança dos ativos de informação do MAPA;

c) a proteção de dados e informações pessoais custodiados pelo MAPA; e

d) o tratamento de informações classificada ou com restrição de acesso;

VI - contribuir para a preservação da memória histórica, cultural e institucional do MAPA;

VII - promover e fomentar a salvaguarda e proteção dos ativos de informação constituintes da cadeia produtiva agropecuária brasileira; e

VIII - contribuir para a consecução da missão e os objetivos estratégicos do MAPA.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 7º As diretrizes gerais da PoSIC/MAPA encontram-se divididas entre os seguintes temas:

I - tratamento da informação;

II - segurança física e do ambiente;

III - gestão de incidentes em segurança da informação;

IV - gestão de ativos;

V - gestão do uso dos recursos operacionais e de comunicação, tais como, e-mail, acesso à internet, mídias sociais, computação em nuvens, dentre outros;

VI - controle de acesso lógico;

VII - gestão de riscos;

VIII - gestão de continuidade; e

IX - auditoria e conformidade.

Seção I

Do Tratamento da Informação

Art. 8º Toda informação produzida, recepcionada, coletada, armazenada ou custodiada será considerada um ativo pertencente ao MAPA, que deverá promover as medidas de segurança necessárias à integridade, disponibilidade e restrição de acesso às informações pessoais, sensíveis ou não, sigilosas e classificadas, e complementarmente, seus agentes públicos obedecerão às seguintes diretrizes:

I - o exercício do direito fundamental de acesso à informação pública ao cidadão, independentemente de motivação, ressalvadas as hipóteses de restrição legalmente previstas, nos termos da Lei nº 12.527, de 18 de novembro de 2011, regulamentada pelo Decreto nº 7.724, de 16 de maio de 2012;

II - o acesso a informações pessoais será disponibilizado somente ao titular da informação ou ao seu procurador devidamente constituído, mediante comprovação de identidade, nos termos do inciso II do art. 55 e art. 60, parágrafo único, inciso I, do Decreto nº 7.724, de 2012;

III - o tratamento de informações pessoais, sensíveis ou não, será realizado mediante a observância das normas contidas na Lei nº 13.709, de 14 de agosto de 2018; e

IV - o tratamento e armazenamento da informação classificada em qualquer grau de sigilo será realizado em observância aos termos disposto no Decreto nº 7.845, de 14 de novembro de 2012, e às normas complementares editadas pela Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS/MAPA.

Seção II

Da Segurança Física e do Ambiente

Art. 9º A segurança física e do ambiente será exercida por meio da combinação de ações de segurança orgânica e utilização de sistema de proteção física com a finalidade de assegurar as condições necessárias à prevenção de incidentes que possam afetar ativos, especialmente, físicos, serviços e agentes públicos do MAPA, durante o exercício de suas atribuições, e obedecerá às seguintes diretrizes:

I - os agentes públicos do MAPA devem seguir as normas vigentes relacionadas à segurança física e patrimonial, sob pena de responsabilidade administrativa;

II - as Unidades do MAPA deverão conservar suas instalações físicas de forma a manter a edificação em condições adequadas ao seu perfeito funcionamento, minimizando eventuais ocorrências de casos fortuitos ou de força maior que possam causar danos ao MAPA; e

III - o cadastro, a entrada, a permanência, a circulação e a saída de pessoas nas instalações dos edifícios sede e anexo do MAPA serão monitorados e controlados pela área de vigilância da unidade, por meio do sistema de "controle de acesso" ou, ainda, por circuito fechado de câmeras, conforme definido em regulamentação interna da área de logística do MAPA.

Seção III

Da Gestão de Incidentes em Segurança da Informação

Art. 10. A área de tecnologia da informação deverá constituir uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, com a responsabilidade de receber, analisar e responder as notificações e as atividades relacionadas a incidentes de segurança em redes de computadores.

Parágrafo único. As normas, padrões e procedimentos técnicos para a atuação da ETIR serão fixados em documento específico a ser elaborado pela área de tecnologia da informação com a participação do Comitê de Segurança da Informação - CSI/MAPA.

Seção IV

Da Gestão de Ativos

Art. 11. A gestão de ativos de informação, compreenderá o processo de inventário e mapeamento destes ativos, com o objetivo de estruturar e manter uma base de dados que sirva de subsídio para os demais processos do MAPA, em especial, os de gestão de risco e de gestão de continuidade em segurança da informação, e obedecerá às seguintes diretrizes:

I - alinhamento aos objetivos estratégicos do MAPA;

II - consideração dos processos internos do MAPA;

III - observância dos requisitos legais e normativos; e

IV - adequação à estrutura do MAPA.

Seção V

Da Gestão do Uso dos Recursos Operacionais e de Comunicações, tais como, e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros

Art. 12. A gestão do uso dos recursos operacionais e de comunicação, especialmente e-mail, acesso à internet, mídias sociais e computação em nuvem, será objeto de atos normativos complementares, a serem editados pela área da tecnologia da informação do MAPA, com a participação do CSI/MAPA.

Parágrafo único. No caso específico de mídias sociais, além do contido no Código de Conduta Ética dos Agentes Públicos do MAPA, poderão ser editadas, a partir de proposta discutida no âmbito do CSI/MAPA, outras normas de conduta para seu uso seguro por parte de seus agentes públicos, cabendo-lhes a responsabilidade por sua observância e cumprimento integrais.

Seção VI

Controles de Acesso Lógico

Art. 13. A área de tecnologia da informação deverá implementar controles e sistematizar a concessão de acesso lógico aos ativos de informação.

Parágrafo único. As normas, padrões e procedimentos técnicos para a implementação de controles e concessão de acesso lógico aos ativos de tecnologia da informação serão fixados em documento específico, a ser elaborado pela área de tecnologia da informação com a participação do CSI/MAPA.

Seção VII

Gestão de Riscos

Art. 14. A gestão de riscos em segurança da informação é o processo de identificar, analisar, avaliar, tratar, registrar, monitorar e comunicar potenciais eventos ou situações visando dar razoável certeza quanto ao alcance dos objetivos da instituição e estará alinhada à Política de Gestão de Riscos e Controles Internos - PGRCI/MAPA.

Art. 15. A gestão de riscos deve promover a adequação entre investimentos em medidas de proteção para minimizar ou eliminar riscos a que estejam sujeitos os ativos de informação do MAPA e os custos dos ativos a serem protegidos.

Seção VIII

Gestão de Continuidade

Art. 16. A gestão de continuidade almeja minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do MAPA, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, e obedecerá às seguintes diretrizes:

I - identificação de atividades críticas;

II - elaboração de planos de gestão de continuidade relacionados às atividades críticas;

III - realização de testes e exercícios dos planos de gestão de continuidade das atividades críticas;

IV - avaliação e aprimoramento dos planos de gestão de continuidade das atividades críticas a partir dos resultados de testes e exercícios;

V - administração da contingência, quando da interrupção de atividades, com base nos planos desenvolvidos; e

VI - proposição de recursos necessários para a implantação e desenvolvimento de ações relacionadas à continuidade das atividades, bem como para a realização dos testes e dos exercícios dos planos.

§ 1º A gestão de continuidade poderá envolver ações mais abrangentes do que as relacionadas à segurança da informação, especialmente devido aos requisitos de continuidade referentes a ativos do MAPA, cabendo às respectivas áreas elaborarem seus planos de continuidade, de acordo com a legislação vigente.

§ 2º As normas, padrões e procedimentos técnicos específicos para a implantação do processo de gestão de continuidade das atividades críticas de tecnologia da informação serão fixados em documento específico, a ser elaborado pela área de tecnologia da informação e deverá contar com a participação do CSI/MAPA.

Seção IX

Auditoria e Conformidade

Art. 17. A auditoria em segurança da informação, observadas as normas, padrões e procedimentos técnicos específicos fixados pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, consistirá na averiguação periódica das ações de segurança da informação referentes aos temas mencionados nos incisos I a VIII do art. 7º deste Anexo, e obedecerá às seguintes diretrizes:

I - aperfeiçoamento constante das ações de segurança da informação por meio da efetiva implementação da PoSIC/MAPA;

II - periodicidade condizente com a política de atualização definida no art. 24; e

III - observância das melhores práticas, nacionais e internacionais, de auditoria em segurança da informação.

Art. 18. A avaliação de conformidade em segurança da informação, observadas as normas, padrões e procedimentos técnicos específicos fixados pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, consistirá em sistemática verificação do adequado grau de confiança nos processos de gestão da segurança da informação, com vistas a evitar desconformidades em relação a requisitos técnicos previamente definidos.

CAPÍTULO VI

DAS COMPETÊNCIAS

Art. 19. Ao Comitê de Governança, Riscos e Controle do Ministério da Agricultura, Pecuária e Abastecimento - CGRC/MAPA compete:

I - promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas a atender as diretrizes gerais de segurança da informação;

II - monitorar o desempenho e avaliar a concepção, a implementação e os resultados da PoSIC/MAPA e de suas instruções normativas complementares;

III - incorporar padrões elevados de conduta para a garantia da segurança da informação e orientar o comportamento dos agentes públicos, em consonância com as funções e atribuições;

IV - planejar a execução de programas, de projetos e de processos relativos à segurança da informação;

V - estabelecer diretrizes para o processo de gestão de riscos de segurança da informação, implementando controles internos correspondentes;

VI - assegurar a implantação de mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados ou contratados;

VII - assegurar a implementação e manutenção de mecanismos, instâncias e práticas de governança da segurança da informação, em consonância com a legislação vigente;

VIII - observar a Política Nacional de Segurança da Informação - PNSI; e

IX - garantir recursos orçamentários para ações de segurança da informação.

Art. 20. Compete ao CSI/MAPA:

I - promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação;

II - supervisionar as atividades desempenhadas pela Equipe de Tratamento e Resposta a Incidentes Cibernéticos em redes computacionais;

III - coordenar e executar as ações de segurança da informação no âmbito de sua atuação;

IV - consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de segurança da informação;

V - assessorar a implementação das ações de segurança da informação;

VI - propor a constituição de grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

VII - elaborar a PoSIC/MAPA e as normas internas de segurança da informação;

VIII - propor alterações à PoSIC/MAPA e às normas internas de segurança da informação; e

IX - deliberar sobre normas internas de segurança da informação.

Art. 21. Ao Gestor de Segurança da Informação compete:

I - assessorar os órgãos específicos singulares do MAPA na implementação da PoSIC/MAPA;

II - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

III - promover a divulgação da política e das normas internas de segurança da informação do Órgão a todos os agentes públicos do MAPA;

IV - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;

V - propor recursos necessários às ações de segurança da informação;

VI - acompanhar os trabalhos da Equipe de Tratamento e Resposta a Incidentes Cibernéticos;

VII - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação; e

VIII - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

CAPÍTULO VII

DAS PENALIDADES

Art. 22. A não observância do disposto na PoSIC/MAPA e nos seus atos normativos complementares acarretará responsabilização administrativa, civil e penal, na forma da legislação vigente.

CAPÍTULO VIII

DA POLÍTICA DE ATUALIZAÇÃO

Art. 23. A PoSIC/MAPA e seus atos normativos complementares deverão ser revisados sempre que se fizer necessário, não excedendo o prazo máximo de 4 (quatro) anos.

CAPÍTULO VIII

DISPOSIÇÕES FINAIS

Art. 24. Todos os agentes públicos do MAPA devem conhecer e zelar pelo cumprimento da PoSIC/MAPA e adotar comportamento seguro, proativo e engajado no que diz respeito à segurança da informação, de acordo com o Código de Conduta Ética dos Agentes Públicos do MAPA.