MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO

Gabinete do Ministro

Portaria GAB/GM/MAPA nº 499, de 17 de outubro de 2022

O **MINISTRO 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 Decreto nº 9.637, de 26 de dezembro de 2018, na Instrução Normativa nº 1, de 27 de maio de 2020, na Instrução Normativa nº 3, de 28 de maio de 2021, ambas do Gabinete de Segurança Institucional da Presidência da República, na Portaria MAPA nº 136, de 25 de maio de 2021, e o que consta do Processo nº 21000.031775/2022-11, resolve:

Art. 1º Fica aprovada, no âmbito do Ministério da Agricultura, Pecuária e Abastecimento, a Política de Gestão de Vulnerabilidades Cibernéticas, na forma do Anexo desta Portaria.

Art. 2º Esta Portaria entra em vigor em 1º de novembro de 2022.

MARCOS MONTES

ANEXO

POLÍTICA DE GESTÃO DE VULNERABILIDADES CIBERNÉTICAS DO MINISTÉRIO DA AGRICULTURA, PECUÁRIA E ABASTECIMENTO

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Seção I

Da finalidade

Art. 1º A Política de Gestão de Vulnerabilidades Cibernéticas tem como finalidade identificar, avaliar, tratar e monitorar vulnerabilidades do ambiente cibernético do Ministério da Agricultura, Pecuária e Abastecimento, tendo como perspectiva a possibilidade de sua exploração por atacantes externos ou internos do qual resulte risco para um ou mais sistemas.

Parágrafo único. Para fins desta Portaria serão considerados os conceitos constantes do Glossário de Segurança da Informação, de que trata a Portaria GSI/PR nº 93, de 18 de outubro de 2021, da Política de Segurança da Informação - PoSIC/MAPA, aprovada pela Portaria MAPA nº 136, de 25 de maio de 2021, e do Código de Conduta

Ética dos Agentes Públicos do Ministério da Agricultura, Pecuária e Abastecimento, aprovado pela Portaria nº 249, de 22 de fevereiro de 2018.

Seção II

Da abrangência

Art. 2º A Política de Gestão de Vulnerabilidades Cibernéticas abrangerá todos os órgãos de assistência direta e imediata ao Ministro de Estado da Agricultura, Pecuária e Abastecimento, os órgãos específicos singulares e os órgãos colegiados, conforme disposto, respectivamente, nos incisos I, II e III do art. 2º do Anexo I do Decreto nº 10.827, de 30 de setembro de 2021.

§ 1º Os contratos firmados pelo Ministério da Agricultura, Pecuária e Abastecimento deverão conter cláusulas que determinem a observância desta Política de Gestão de Vulnerabilidades Cibernéticas por parte do contratado e de seus dirigentes, prepostos, administradores, representantes e colaboradores.

§ 2º As entidades vinculadas, de que trata o inciso IV do art. 2º do Anexo I do Decreto nº 10.827, de 2021, deverão editar suas respectivas políticas de gestão de vulnerabilidades cibernéticas.

CAPÍTULO II

DOS OBJETIVOS

Art. 3º São objetivos da Política de Gestão de Vulnerabilidades Cibernéticas:

I - fornecimento de subsídios ao planejamento e à implementação do gerenciamento de riscos em segurança da informação;

II - obtenção de informações confiáveis sobre vulnerabilidades descobertas em soluções de Tecnologia da Informação - TI;

III - identificação das vulnerabilidades existentes no ambiente cibernético do Ministério da Agricultura, Pecuária e Abastecimento;

IV - classificação e priorização das vulnerabilidades identificadas;

V - adoção de controle, monitoramento e mitigação para minimizar o impacto ou a probabilidade de exploração das vulnerabilidades mais relevantes; e

VI - promoção da capacidade de resiliência cibernética.

CAPÍTULO III

DOS PRÉ-REQUISITOS DA GESTÃO DE VULNERABILIDADES CIBERNÉTICAS

Seção I

Do escopo

Art. 4º A Política de Gestão de Vulnerabilidades Cibernéticas será supervisionada pelo Comitê de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento - CSI/MAPA e operacionalizada pelo Departamento de Tecnologia da Informação da Secretaria-Executiva do Ministério da Agricultura, Pecuária e Abastecimento.

§ 1º Para operacionalizar a Política de Gestão de Vulnerabilidades Cibernéticas, o Departamento de Tecnologia da Informação deverá definir escopo apropriado à quantidade de ativos de informação, hardware e software, e priorizar o Plano Estratégico vigente e os serviços considerados críticos.

§ 2º Fazem parte do escopo de que trata o § 1º do **caput**, por ordem ascendente de criticidade:

I - vulnerabilidades expostas à internet;

II - vulnerabilidades de fácil exploração;

III - vulnerabilidades em ativos de infraestrutura crítica de Tecnologia da Informação - TI; e

IV - vulnerabilidades massivas.

Seção II

Do inventário

Art. 5º Deverá ser mantido atualizado o inventário completo dos ativos de informação sob a gestão do Departamento de Tecnologia da Informação, como pré-requisito para a gestão efetiva das vulnerabilidades técnicas, o qual identificará, no mínimo, todos os ativos de **hardware** e **software**.

CAPÍTULO IV

DA EXECUÇÃO DA GESTÃO DE VULNERABILIDADES CIBERNÉTICAS

Seção I

Da identificação de vulnerabilidades

Art. 6º A critério do Departamento de Tecnologia da Informação serão realizadas varreduras periódicas em todo ambiente cibernético, de forma automatizada ou por meio de análise humana, para identificar vulnerabilidades sob a perspectiva de atacantes externos e internos.

Parágrafo único. As varreduras periódicas externas e internas, de que trata o **caput**, serão preferencialmente executadas utilizando autenticação para permitir análises mais completas.

Seção II

Da avaliação de vulnerabilidades

Art. 7º As vulnerabilidades identificadas serão registradas minimamente de acordo com os seguintes critérios:

I - utilização da métrica internacional **Common Vulnerability Scoring System (CVSS)**, que fornece uma representação numérica de zero a dez, relativa à gravidade da vulnerabilidade; e

II - identificação quanto à existência de programa ou código projetado para explorar a vulnerabilidade identificada (**exploit**).

Art. 8º As vulnerabilidades serão classificadas conforme a criticidade estabelecida nos incisos I a IV do § 2º do art. 4º desta Portaria, e priorizadas em matriz cujos critérios sejam de gravidade, urgência, tendência e esforço.

Art. 9º As vulnerabilidades identificadas, classificadas e priorizadas constarão de base de dados local oriundas das principais vulnerabilidades cibernéticas, para fins de acompanhamento e comunicação à alta administração.

Seção III

Do tratamento de vulnerabilidades

Art. 10. Na base de dados das principais vulnerabilidades cibernéticas deverão ser registrados:

I - o responsável;

II - a causa-raiz; e

III - o prazo para remediação ou tratamento.

Art. 11. Em relação ao tratamento das vulnerabilidades serão observados:

I - o processo de tratamento e resposta a incidentes de segurança;

II - a realização de testes e homologação da correção da vulnerabilidade técnica antes da aplicação em ambiente de produção; e

III - se as alterações de configuração no ambiente, motivadas pelas correções das vulnerabilidades técnicas, foram implantadas de acordo com o processo de gestão de mudanças.

Parágrafo único. A ação de tratamento referente a cada vulnerabilidade identificada, na forma do disposto no **caput**, consistirá em:

I - mudança da configuração no ambiente;

II - aplicação da solução de contorno;

III - implantação de solução ou serviço; e

IV - aceitação do risco.

Seção IV

Do monitoramento de vulnerabilidades

Art. 12. Caberá ao Departamento de Tecnologia da Informação produzir informações sobre vulnerabilidades e a aplicação da(s) medida(s) de segurança recomendada(s), as quais deverão ser submetidas periodicamente ao conhecimento do Comitê de Segurança da Informação.

Parágrafo único. São fontes de consulta preferenciais:

I - vulnerabilidades divulgadas pelos fabricantes das soluções de Tecnologia da Informação utilizadas no Ministério da Agricultura, Pecuária e Abastecimento;

II - vulnerabilidades divulgadas por fabricantes e empresas especializadas em segurança da informação;

III - boletins de equipes governamentais de resposta a incidentes;

IV - fóruns e sites especializados;

V - comunicações de usuários; e

VI - outras fontes que vierem a surgir.

Art. 13. A critério do Departamento de Tecnologia da Informação, poderão ser aplicados um ou mais dos controles relacionados abaixo, a partir da análise crítica dos resultados da gestão de vulnerabilidades:

I - comparação regular dos tempos de tratamento das vulnerabilidades para verificar se foram corrigidas em tempo hábil;

II - acompanhamento regular do nível geral de risco do ambiente cibernético; e

III - apresentação ao Comitê de Segurança da Informação, a respeito da evolução dos riscos e dos achados dos testes e das varreduras, para fins de proposição de melhorias nos processos da gestão de vulnerabilidades.

CAPÍTULO V

DAS RESPONSABILIDADES E COMPETÊNCIAS

Art. 14. Para assegurar a rastreabilidade adequada das vulnerabilidades, as responsabilidades e competências da Política de Gestão de Vulnerabilidades Cibernéticas de que trata esta Portaria serão segregadas, observados os seguintes parâmetros:

I - as áreas responsáveis pela administração de soluções de Tecnologia da Informação deverão monitorar as vulnerabilidades disponibilizadas pelos fabricantes das soluções e aplicar as respectivas atualizações de segurança (**patch management**);

II - a área de Tecnologia da Informação será responsável pela varredura e classificação de vulnerabilidades cibernéticas, por monitorar fontes de consulta relacionadas a vulnerabilidades cibernéticas e medidas de tratamento, pelo acompanhamento do tratamento das vulnerabilidades e pela análise crítica e proposição de melhorias no processo de gestão de vulnerabilidades; e

III - a unidade de Infraestrutura da área de Tecnologia da Informação será encarregada de aplicar regularmente as atualizações de segurança dos sistemas operacionais e, centralmente, atualizar os aplicativos instalados nas estações de trabalho.

Parágrafo único. O Comitê de Segurança da Informação deverá ser informado, no mínimo em uma reunião ordinária, sobre as ações implementadas pelo Departamento de Tecnologia da Informação para identificação, avaliação e tratamento das vulnerabilidades identificadas, conforme dispõe os arts. 6º a 11 desta Portaria, de modo que o Colegiado ratifique, em todo ou parcialmente, as ações de tratamento e monitoramento das vulnerabilidades priorizadas no âmbito do Ministério da Agricultura, Pecuária e Abastecimento.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 15. Os relatórios e registros gerados a partir da publicação desta Portaria serão tratados e armazenados de forma segura e com acesso reservado às Unidades envolvidas.

Art. 16. Os casos omissos deverão ser submetidos ao Comitê de Segurança da Informação do Ministério da Agricultura, Pecuária e Abastecimento, para conhecimento e deliberação.

MARCOS MONTES
Ministro de Estado da Agricultura, Pecuária e Abastecimento
