MINISTÉRIO DOS DIREITOS HUMANOS E DA CIDADANIA

PORTARIA Nº 742, DE 27 DE NOVEMBRO DE 2023

Institui a Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania.

O MINISTRO DE ESTADO DOS DIREITOS HUMANOS E DA CIDADANIA, no uso da atribuição que lhe confere o inciso II do parágrafo único do art. 87 da Constituição, e tendo em vista o disposto no inciso II do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018, nos incisos do art. 3º e no inciso VIII do art. 5º da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, resolve:

CAPÍTULO I

DO ESCOPO

Art. 1º Instituir a Política de Segurança da Informação, no âmbito do Ministério dos Direitos Humanos e da Cidadania, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações de segurança da informação e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas.

§ 1º Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania são parte integrante desta Política e emanam dos princípios e diretrizes nela estabelecidos.

§ 2º A estrutura da Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania é integrada por três instrumentos normativos, de níveis hierárquicos distintos, quais sejam:

I - política de segurança da informação, documento obrigatório que define a estrutura, as diretrizes e as obrigações referentes à segurança da informação que devem ser seguidas;

II - normas internas de segurança da informação, documentos que identificam as regras básicas de como devem ser implementados os controles definidos pela POSIN; e

III - procedimentos de segurança da informação, documentos que instrumentalizam as normas internas, permitindo a direta aplicação nas atividades do Ministério dos Direitos Humanos e da Cidadania.

§ 3º As diretrizes de segurança da informação previstas nesta Política e nas demais normas específicas de segurança da informação do Órgão são aplicadas a todos os colaboradores, conforme definição dada no Anexo I, que tenham acesso às informações e aos recursos de Tecnologia da Informação deste Ministério.

Art. 2º A Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania tem como objetivos:

I - nortear a elaboração das normas necessárias à efetiva implementação da segurança da

informação;

II - estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

III - estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações; e

IV - estabelecer competências e responsabilidades quanto à segurança da informação.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º As ações de segurança da informação do Ministério dos Direitos Humanos e da Cidadania são orientadas pelos princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como pelos seguintes princípios:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações;

II - continuidade dos processos e serviços essenciais para o funcionamento do Ministério;

III - responsabilidade dos colaboradores, constituída no dever de conhecer e respeitar a Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania e demais normas específicas de segurança da informação do Órgão;

IV - alinhamento estratégico da Política e Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania com o planejamento estratégico do Órgão, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

V - conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis;

VI - educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação;

VII - clareza, no sentido de que as regras que se fundam nesta política devem ser claras, objetivas e concisas, a fim de viabilizar sua fácil compreensão;

VIII - publicidade, transparência às informações, respeitando a privacidade do cidadão;

IX - auditabilidade, no sentido que todos os eventos significativos dos processos e sistemas devem ser rastreáveis até o evento inicial, identificando, inclusive, o responsável pelo seu acontecimento;

X - resiliência, significando que os processos, sistemas e controles devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre; e

XI - substituição da segurança em situações de emergência, ou seja, os controles de segurança devem ser desconsiderados somente de formas pré-determinadas e seguras, devendo existir procedimentos e controles alternativos previamente elencados para minimizar o nível de risco em situações de emergência.

CAPÍTULO III

DAS DIRETRIZES GERAIS

Art. 4º Estas diretrizes constituem os principais pilares da gestão de segurança da informação no Ministério dos Direitos Humanos e da Cidadania, norteando a elaboração de políticas, planos e normas complementares no âmbito deste Ministério e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 5º As normas, procedimentos, manuais e metodologias de segurança da informação

do Ministério devem considerar, como referência, além das citadas no Anexo II, as melhores práticas de segurança da informação.

Art. 6º As ações de segurança da informação devem:

I - considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do Órgão;

II - ser tratadas de forma integrada, respeitando as especificidades e autonomia das unidades do Ministério;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV - visar à prevenção da ocorrência de incidentes.

Art. 7º O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos para o Ministério.

Art. 8º Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no Ministério dos Direitos Humanos e da Cidadania compõe o seu ativo da informação e deve ser protegida conforme normas em vigor estabelecidas no âmbito do Órgão, e, no que couber, conforme normativos constantes do Anexo II.

Art. 9º As pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação do Órgão a assinatura de Termo de Responsabilidade ou Termo de Ciência, contendo ciência aos termos desta Política, as responsabilidades e compromissos em decorrência deste acesso e penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação do Ministério dos Direitos Humanos e da Cidadania.

Art. 10. Esta Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do Ministério dos Direitos Humanos e da Cidadania, deverão ser divulgadas amplamente a todos os colaboradores, ainda que a atuação no Órgão seja temporária, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os colaboradores devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no parágrafo anterior deverão ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 11. Todos os contratos de prestação de serviços, firmados pelo Ministério dos Direitos Humanos e da Cidadania conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política de Segurança da Informação.

Art. 12. A estrutura do Sistema de Gestão de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania será definida em norma específica.

§ 1º A estrutura prevista no caput deverá, contemplar em sua composição, ao menos:

I - o Gestor de Segurança da Informação do Órgão;

II - a(s) equipe(s) de tratamento e resposta a incidentes em redes computacionais; e

III - os comitês e subcomitês de segurança da informação.

§ 2º A Política de Segurança da Informação integra o arcabouço legal do Sistema de Gestão de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania.

§ 3º A estrutura do Sistema de Gestão de Segurança da Informação do Ministério dos

Direitos Humanos e da Cidadania deverá estar em conformidade com o modelo de governança do Ministério dos Direitos Humanos e da Cidadania.

CAPÍTULO IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 13. A alta administração do Ministério dos Direitos Humanos e da Cidadania deve se comprometer com o desenvolvimento e com a implementação do Sistema de Gestão de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados.

Art. 14. Cabe ao Comitê de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania:

I - estabelecer, regulamentar e rever, quando necessário, os princípios e diretrizes desta Política, promover a implementação das ações preventivas e corretivas de segurança da informação, de forma sistêmica e integrada aos negócios, e respaldar a realização de auditorias, dentre outras competências previstas em seu regimento; e

II - estabelecer normas e procedimentos destinados a disciplinar e proteger o uso da informação no âmbito do Ministério, complementando a Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania, sobre, dentre outros que julgar pertinente, os seguintes temas julgados relevantes para a sua atuação:

a) Tratamento da Informação;

b) Segurança Física e do Ambiente;

c) Gestão de Incidentes em Segurança da Informação;

d) Gestão de Ativos;

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

f) Controles de Acesso;

g) Gestão de Risco;

h) Gestão de Continuidade;

i) Auditoria e Conformidade;

j) Criptografia; e

k) Desenvolvimento Seguro de Software.

Art. 15. É responsabilidade de todos os gestores do Ministério o conhecimento e a disseminação desta Política e demais normas específicas de segurança da informação do Órgão aos colaboradores que estão sob a sua gestão.

Art. 16. Todos os colaboradores são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 17. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas de ofício às instâncias superiores, assim que identificadas.

Art. 18. A Política de Segurança da Informação, demais normas internas e procedimentos complementares têm abrangência universal, e devem ser cumpridas por todos os servidores, colaboradores, estagiários, consultores externos e prestadores de serviço que exerçam atividades no âmbito do Ministério dos Direitos Humanos e da Cidadania ou quem quer que tenha acesso a dados ou informações no ambiente do Ministério.

CAPÍTULO V

DAS PENALIDADES

Art. 19. Ações que violem a Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VI

DA ATUALIZAÇÃO

Art. 20. A Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania deverá ser revisada em função de alterações na legislação pertinente, de diretrizes políticas do Governo Federal, de alterações nos normativos do Órgão, quando considerada necessária pelo Comitê de Segurança da Informação, ou a cada doze meses a contar da data de sua publicação.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 21. Os órgãos integrantes do Sistema de Gestão de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos relativos à segurança da informação alinhados às diretrizes emanadas pelo Comitê de Segurança da Informação e aos respectivos Planos Estratégicos Institucionais desses órgãos.

Art. 22. As dúvidas sobre a Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania e seus documentos devem ser submetidas ao Comitê Estratégico de Segurança da Informação.

Art. 23. Aplicam-se a esta Política de Segurança da Informação, no que couber, as disposições da Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, e da Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011.

Art. 24. Esta Portaria entra em vigor na data de sua publicação.

SILVIO LUIZ DE ALMEIDA

Documento assinado eletronicamente por **Silvio Luiz de Almeida**, **Ministro de Estado dos Direitos Humanos e da Cidadania**, em 28/11/2023, às 14:52, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020** .

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **3968615** e o código CRC **8B5AFC19**.

ANEXO I

CONCEITOS E DEFINIÇÕES

1. Para os fins da Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania, fica estabelecido o significado dos seguintes termos e expressões:

1.1. Ativo: qualquer coisa que tenha valor para a organização;

1.2. Ativo de informação: o patrimônio composto por todos os dados e informações geradas, custodiadas, manipuladas, utilizadas ou armazenada no Ministério dos Direitos Humanos e da Cidadania, bem assim todos os elementos de pessoal (colaboradores que manuseiam os ativos), infraestrutura, tecnologia, hardware e software necessários à execução dos processos da organização;

1.3. 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;

1.4. Colaborador: todas as pessoas envolvidas com o desenvolvimento de atividades no Ministério dos Direitos Humanos e da Cidadania, de caráter permanente, continuado ou eventual, incluindo autoridades, servidores, prestadores de serviço, consultores e estagiários;

1.5. 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;

1.6. Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

1.7. Conscientização: atividade que tem por finalidade orientar sobre o que é segurança da informação levando os participantes a obterem um nível adequado de conhecimento sobre segurança, além de um senso apropriado de responsabilidade;

1.8. Desastre: evento, ação ou omissão, repentino e não planejado, que tenha permitido acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica, causando perda para toda ou parte da organização e gerando sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;

1.9. Diretrizes de Segurança da Informação: ações que definem a Política de Segurança da Informação do Ministério dos Direitos Humanos e da Cidadania, visando a preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações da Instituição;

1.10. 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;

1.11. Equipe de Tratamento e Resposta a Incidentes cibernéticos (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

1.12. Firewall: recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um a conjunto de redes, ou a partir dela;

1.13. 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;

1.14. Gestão de riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

1.15. Gestão de Segurança da Informação: 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, às tecnologias da informação e comunicação;

1.16. Gestor de Segurança da Informação: servidor público efetivo responsável pelas ações de segurança da informação do Ministério dos Direitos Humanos e da Cidadania;

1.17. Incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

1.18. Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

1.19. Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

1.20. Plano de Continuidade de Negócios: documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;

1.21. Plano de Gerenciamento de Incidentes: plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

1.22. Plano de Tratamento dos Riscos: processo e implementação de ações de segurança da informação para evitar, reduzir, reter ou transferir um risco;

1.23. POSIN: acrônimo de política de segurança da informação;

1.24. Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

1.25. Recurso: é um meio de qualquer natureza (humano, físico, tecnológico, financeiro, de imagem de mercado, de credibilidade, entre outros) que permite alcançar aquilo a que se propõe;

1.26. Recursos de Tecnologia da Informação: conjunto formado pelos bens e serviços de tecnologia da informação que constituem a infraestrutura utilizada na produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação da informação;

1.27. Responsável pelo ativo de informação: servidor público responsável pela salvaguarda do ativo de informação;

1.28. Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade;

1.29. Risco de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

1.30. Segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

1.31. Servidor público: toda pessoa legalmente investida em cargo público;

1.32. Sistema de Gestão de Segurança da Informação: é um conjunto de pessoas, processos e procedimentos, baseado em normas e na legislação vigente, que uma organização deve implementar para prover segurança no uso de seus ativos de informação de modo a preservá-los quanto aos aspectos de disponibilidade, integridade, confidencialidade e autenticidade, independentemente do meio em que se encontram;

1.33. 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;

1.34. 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;

1.35. Tratamento de incidentes: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

1.36. Usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da Administração Pública Federal, formalizada por meio da assinatura de Termo de Responsabilidade; e

1.37. Vulnerabilidades: fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, e podem ser corrigidas ou evitadas por uma ação interna de segurança da informação.

ANEXO II

REFERÊNCIAS LEGAIS E NORMATIVAS

1. Esta norma foi elaborada em conformidade às seguintes referências legais e normativas:

1.1. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020, e suas normas complementares, que disciplinam a Gestão de Segurança da Informação e Comunicação na Administração Pública Federal;

1.2. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

1.3. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

1.4. Lei nº 12.527, de 18 de novembro de 2011, Lei de Acesso à Informação, que regula o acesso a informações;

1.5. Decreto nº 10.332, de 28 de abril de 2020, que institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

1.6. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

1.7. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

1.8. Decreto nº 9.832, de 12 de junho de 2019, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação;

1.9. ABNT NBR ISO/IEC 27001 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação;

1.10. ABNT NBR ISO/IEC 27002 - Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação; e

1.11. ABNT NBR ISO/IEC 27005 - Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação.