DIÁRIO OFICIAL DA UNIÃO

Publicado em: 31/01/2022 | Edição: 21 | Seção: 1 | Página: 193

Órgão: Ministério da Justiça e Segurança Pública/Gabinete do Ministro

PORTARIA MJSP Nº 2, DE 28 DE JANEIRO DE 2022

Institui o Sistema de Governança do Ministério da Justiça e Segurança Pública.

O MINISTRO DE ESTADO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso das atribuições que lhe conferem os incisos I e II do parágrafo único do art. 87 da Constituição, e tendo em vista o disposto no art. 37 da Lei nº 13.844, de 18 de junho de 2019, no art. 1º do Anexo I do Decreto nº 9.662, de 1º de janeiro de 2019, e no Decreto nº 9.203, de 22 de novembro de 2017, e o que consta no Processo Administrativo nº 08011.000086/2021-96, resolve:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Instituir o Sistema de Governança do Ministério da Justiça e Segurança Pública - SG-MJSP, com o objetivo de organizar o processo decisório quanto à gestão estratégica, à gestão de riscos e controles internos, à integridade, à gestão de políticas públicas, à transparência, à gestão administrativa, à gestão de dados e à tecnologia e segurança da informação.

Parágrafo único. A governança do MJSP incorporará os princípios, as diretrizes e os mecanismos definidos na política de governança da administração pública federal direta, autárquica e fundacional, e as recomendações oriundas de manuais, guias e resoluções aprovados pelo Comitê Interministerial de Governança - CIG, nos termos do inciso II do art. 9º do Decreto nº 9.203, de 22 de novembro de 2017.

CAPÍTULO II

DISPOSIÇÕES GERAIS

Art. 2º Para os efeitos do disposto nesta Portaria, considera-se:

I - alta administração: Ministros de Estado, ocupantes dos cargos de Natureza Especial - NE, ocupantes dos cargos de Direção e Assessoramento Superior - DAS ou de Função Comissionada do Poder Executivo - FCPE, níveis 101.6 ou 101.5, que atuam como dirigentes máximos no âmbito dos órgãos específicos singulares e entidades vinculadas ao MJSP;

II - unidades finalísticas: órgãos específicos singulares e entidades vinculadas integrantes da estrutura organizacional do MJSP;

III - governança pública: conjunto de mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a gestão, com vistas à condução de políticas públicas e à prestação de serviços de interesse da sociedade;

IV - política pública: conjunto de ações ou programas governamentais finalísticos necessários, suficientes, integrados e articulados para a provisão de bens ou serviços, dotados de recursos orçamentários ou de recursos oriundos de renúncia de receita ou de benefícios de natureza financeira e creditícia;

V - política pública em fase de elaboração: instituição de política pública que não faça parte da programação governamental vigente, ou agregação e desagregação de políticas públicas já existentes, não tendo recebido dotação orçamentária anteriormente;

VI - política pública em fase de execução: política pública que faça parte da programação governamental vigente, tendo recebido dotação orçamentária no exercício anterior ou no atual;

VII - política pública em fase de ampliação: ação que acarrete o aumento no valor da programação orçamentária ou da renúncia de receitas e de benefícios de natureza financeira e creditícia para ampliar política pública já existente;

VIII - política pública em fase de aperfeiçoamento: alteração no desenho de política pública já existente na programação governamental em execução, podendo ou não ocasionar aumento orçamentário; e

IX - valor público: produtos e resultados gerados, preservados ou entregues pelas atividades de uma organização, que representem respostas efetivas e úteis às necessidades ou às demandas de interesse público e modifiquem aspectos do conjunto da sociedade ou de alguns grupos específicos reconhecidos como destinatários legítimos de bens e serviços públicos.

CAPÍTULO III

DO SISTEMA DE GOVERNANÇA DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Art. 3º O SG-MJSP, caracterizado como o conjunto de práticas gerenciais voltado à entrega de valor público para a sociedade, com a finalidade de estabelecer o modelo de tomada de decisão sobre planejamento estratégico, políticas públicas, integridade, riscos e controles, informação, recursos de tecnologia da informação e comunicação, dados e sistemas de informação, contratações, pessoal e transparência.

Art. 4º São objetivos do SG-MJSP:

I - promover e organizar os mecanismos, instâncias e práticas de governança em consonância com os princípios e as diretrizes estabelecidas na política de governança da administração pública federal direta, autárquica e fundacional;

II - promover a implementação e o monitoramento da gestão estratégica;

III - promover a gestão de políticas públicas em todas as suas fases, conforme disposto nos incisos V a VIII do art. 2º;

IV - promover o processo permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar e gerenciar potenciais eventos de risco que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;

V - promover a adoção de medidas e ações institucionais destinadas à prevenção, detecção e punição de fraudes e atos de corrupção com a aprovação, a implantação e o monitoramento de programa de integridade que utilize a gestão de risco para identificação prévia e tratamento dos riscos;

VI - promover a prestação de contas à sociedade sobre os resultados da atuação do Ministério;

VII - promover mecanismos para ouvir reclamações e sugestões da sociedade;

VIII - controlar a carteira de políticas públicas do Ministério;

IX - promover a implementação da gestão de dados e de sistemas de informações; e

X - promover a segurança da informação e comunicação.

CAPÍTULO IV

DOS ELEMENTOS DA GOVERNANÇA

Art. 5º São elementos da Governança:

I - gestão estratégica;

II - gestão administrativa;

III - gestão de riscos e controles internos;

IV - gestão de integridade;

V - gestão de políticas públicas;

VI - gestão de transparência;

VII - gestão de dados e de sistemas de informações; e

VIII - gestão de tecnologia da informação e comunicação.

Art. 6º A gestão estratégica compreende a definição de diretrizes, objetivos, planos, projetos e ações, além de critérios de priorização e alinhamento entre as partes interessadas, para que os serviços e produtos de responsabilidade do Ministério alcancem o resultado pretendido, nos termos do Anexo X.

Art. 7º A gestão administrativa engloba atividades de suporte, realizadas em apoio à gestão finalística, e envolve a gestão de contratações, contratos, pessoas, informação, gestão de documentos de arquivo, comunicação corporativa, informações organizacionais do Governo Federal, orçamento federal, administração financeira federal e contabilidade federal, nos termos dos Anexos III e VII.

Art. 8º A gestão de riscos e controles internos do Ministério engloba a aplicação sistemática de procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco, nos termos dos Anexos IV e VIII.

Art. 9º A gestão de integridade do Ministério engloba atividades institucionais voltadas para a prevenção, a detecção e a punição de desvios éticos, as fraudes e os atos de corrupção, em apoio à boa governança, nos termos dos Anexos V e IX.

Art. 10. A gestão de políticas públicas envolve a sua estruturação em uma Carteira de Políticas Públicas, para permitir o monitoramento, a avaliação e a alocação orçamentária pela alta gestão, promovendo a tomada de decisão baseada em evidências, contribuindo para a melhoria da qualidade do gasto, para a racionalização do uso de recursos públicos e para a difusão da cultura da transparência, nos termos do Anexo XI.

Art. 11. A gestão de transparência e acesso à informação do Ministério busca promover o direito constitucional dos cidadãos de acessar informações públicas de interesse particular ou coletivo, produzidas ou acumuladas pelo Ministério, observado o disposto na Lei nº 12.527, de 18 de novembro de 2011, na Lei nº 13.709, de 14 de agosto de 2018, no Decreto nº 7.724, de 16 de maio de 2012, e na Resolução nº 11, de 11 de dezembro de 2017, da Comissão de Ética Pública.

Art. 12. A gestão de dados e sistemas de informações contempla o conjunto de práticas gerenciais, mecanismos de liderança, estratégias e controles, instituídos com a finalidade de estabelecer o modelo de tomada de decisão nos assuntos relacionados à gestão, ao compartilhamento, à transparência e abertura de dados, às informações e aos sistemas de informação.

Art. 13. A gestão de tecnologia da informação e comunicação abrange o conjunto de controles, práticas e processos de suporte ao gerenciamento dos recursos de tecnologia da informação e comunicação com a finalidade de alcançar os objetivos estabelecidos pelo Ministério para a área, incluindo aqueles relacionados à segurança da informação digital.

Parágrafo único. A gestão mencionada no caput é exercida pelo órgão setorial do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) e, nas unidades vinculadas, pelos órgãos correlatos.

Art. 14. Ficam criados:

I - o Comitê de Governança Estratégica - CGE, nos termos do Anexo I;

II - a Comissão Técnica do Comitê de Governança Estratégica - CT-CGE, nos termos do Anexo II;

III - o Comitê de Governança Administrativa - CGA, nos termos do Anexo III;

IV - as Instâncias de Supervisão de Gestão de Riscos e Controles Internos, nos termos do Anexo IV;

V - a Comissão Executiva do Programa de Integridade do MJSP - CEPI, nos termos do Anexo V;

VI - o Comitê de Governança de Dados e Sistemas de Informação - CGDI, nos termos do Anexo VI;

VII - o Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC, nos termos do Anexo VII;

VIII - a Política de Gestão de Riscos e Controles Internos - PGRCI, nos termos do Anexo VIII;

IX - o Programa de Integridade do MJSP, nos termos do Anexo IX;

X - o Processo de Gestão Estratégica, nos termos do Anexo X;

XI - o Processo de Gestão de Políticas Públicas, nos termos do Anexo XI;

XII - a Política de Governança de Dados e Sistemas de Informação do MJSP - PGDS, nos termos do Anexo XII; e

XIII - a Política de Segurança da Informação e Comunicação - POSIC, nos termos do Anexo XIII.

Art. 15. Integram o SG-MJSP:

I - o Comitê de Governança Estratégica - CGE;

II - a Comissão Técnica do Comitê de Governança Estratégica - CT-CGE;

III - o Comitê de Governança Administrativa - CGA;

IV - a Comissão Executiva do Programa de Integridade MJSP - CEPI;

V - as Instâncias de Supervisão de Gestão de Riscos e Controles Internos;

VI - o Comitê de Governança de Dados e Sistemas de Informação - CGDI;

VII - o Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC.

Art. 16. O SG-MJSP será conduzido pelo CGE, com o apoio dos comitês, comissões e instâncias listados no art. 14 e no art. 15.

§ 1º O CGE será a instância máxima do SG-MJSP para avaliar e aprovar as iniciativas de gestão estratégica, de gestão de riscos e controles internos, de gestão de transparência, de gestão de integridade, de gestão de políticas públicas, de gestão administrativa, e de gestão de dados e sistemas de informação e de gestão da tecnologia da informação e comunicações.

§ 2º A CT-CGE funcionará como unidade de apoio executivo do CGE para temas relacionados com as atividades finalísticas do Ministério, de modo a acompanhar resultados e a identificar pontos que necessitem de deliberação pelo CGE.

§ 3º O CGA funcionará como unidade de apoio executivo do CGE para temas relacionados com as atividades de suporte do Ministério, de modo a acompanhar resultados e a identificar pontos que necessitem de deliberação pelo CGE.

§ 4º A CEPI funcionará como unidade de apoio executivo do CGE para temas relacionados com as atividades de integridade do Ministério, de modo a acompanhar resultados e a identificar pontos que necessitem de deliberação pelo CGE.

§ 5º O Comitê de Gestão de Riscos e Controles Internos - CGRC, que integra as instâncias de supervisão de gestão de riscos e controles internos, funcionará como unidade de apoio executivo do CGE para temas relacionados com as atividades de gestão de riscos do Ministério, de modo a acompanhar resultados e a identificar pontos que necessitem de deliberação pelo CGE.

§ 6º O CGDI funcionará como unidade de apoio executivo do CGE para temas relacionados à governança de dados e sistemas de informação, automatizados ou não automatizados.

§ 7º O CGDSIC funcionará como unidade de apoio do CGE para temas relacionados com a gestão de tecnologias de informação e comunicação e gestão de segurança da informação e comunicação do Ministério, de modo a acompanhar resultados e a identificar pontos que necessitem de deliberação pelo CGE.

Art. 17. Ficam revogadas:

I - a Portaria MJ nº 3.530, de 3 de dezembro de 2013; e

II - a Portaria MJSP nº 86 de 23 de março de 2020.

Art. 18. Esta Portaria entra em vigor na data de sua publicação.

ANDERSON GUSTAVO TORRES

ANEXO I

COMITÊ DE GOVERNANÇA ESTRATÉGICA

Art. 1º Compete ao Comitê de Governança Estratégica - CGE:

I - definir as diretrizes estratégicas do Ministério;

II - promover o alinhamento e a convergência do planejamento estratégico do Ministério com as diretrizes estratégicas;

III - promover revisões no planejamento estratégico do Ministério, quando necessário;

IV - promover o alinhamento das diretrizes estratégicas com as ações relacionadas à gestão de dados e sistemas de informação, de tecnologia da informação e comunicação, de segurança da informação e comunicação, de riscos, de governança, de processos, de projetos, de pessoas, orçamentária, financeira, contábil e com a Estratégia de Governança Digital - EGD;

V - aprovar e institucionalizar o plano de comunicação do planejamento estratégico;

VI - apreciar matérias diversas de relevância estratégica;

VII - monitorar os objetivos, os projetos, os indicadores e as metas integrantes do planejamento estratégico;

VIII - aprovar a carteira de políticas públicas;

IX - aprovar e promover práticas e princípios de conduta e padrões de comportamento;

X - apoiar a inovação e a adoção de boas práticas de gestão de governança, de riscos e controles internos e de integridade;

XI - promover a observância dos códigos, leis, normas e padrões na condução das políticas e na prestação de serviços de interesse público;

XII - estabelecer a aplicação de boas práticas de gestão de governança, de riscos, integridade e controle interno;

XIII - promover a adoção de práticas que institucionalizem a responsabilidade dos agentes públicos na prestação de contas, transparência e efetividade das informações;

XIV - promover a integração e o desenvolvimento contínuo dos agentes responsáveis pela gestão de riscos e controles internos e pela gestão de integridade;

XV - aprovar políticas, diretrizes, metodologias, manuais e mecanismos de monitoramento e comunicação para gestão de riscos e controles internos;

XVI - definir ações para disseminação da cultura de gestão estratégica, administrativa, de riscos e controles internos, de integridade, de políticas públicas, de transparência e de dados e sistemas de informação;

XVII - aprovar método de priorização de processos para a gestão de riscos e controles internos;

XVIII - aprovar as categorias de riscos a serem gerenciados;

XIX - estabelecer os limites de exposição a riscos e níveis de conformidade;

XX - estabelecer os limites de tolerância a riscos dos órgãos de assistência direta e imediata ao Ministro e dos órgãos específicos singulares;

XXI - aprovar o modelo de supervisão da gestão de riscos e controles internos;

XXII - aprovar o plano de implementação de controles elaborado pelos órgãos do Ministério contendo as medidas mitigadoras dos riscos que possam comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público;

XXIII - tomar decisões com base em informações sobre a gestão de riscos e controles internos, assegurando que estejam disponíveis em todos os níveis;

XXIV - emitir recomendações e orientações para o aprimoramento da gestão de riscos e controles internos;

XXV - aprovar o Plano de Ação referente à gestão de integridade;

XXVI - praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades; e

XXVII - aprovar o seu regimento interno e suas alterações.

Parágrafo único. As decisões e diretrizes aprovadas pelo CGE serão formalizadas por meio da publicação de Resoluções do Comitê de Governança Estratégica no Boletim de Serviço do MJSP.

Art. 2º O CGE será composto pelos seguintes membros:

I - Ministro de Estado da Justiça e Segurança Pública, que o presidirá;

II - Chefe de Gabinete do Ministro de Estado da Justiça e Segurança Pública;

III - Chefe da Assessoria Especial de Controle Interno;

IV - Secretário-Executivo;

V - Secretário-Executivo Adjunto;

VI - Subsecretário de Administração;

VII - Subsecretário de Planejamento e Orçamento;

VIII - Diretor de Tecnologia da Informação e Comunicação;

IX - Ouvidor Geral; e

X - Alta administração dos órgãos específicos singulares e entidades vinculadas ao Ministério.

Parágrafo único. Nas ausências e impedimentos do Ministro de Estado da Justiça e Segurança Pública, o CGE será presidido pelo seu substituto legal e, na sua ausência, pelo Secretário-Executivo substituto.

Art. 3º O apoio administrativo ao CGE caberá à Coordenação-Geral de Gestão Estratégica e Inovação Institucional - CGGE, sob supervisão do Subsecretário de Planejamento e Orçamento da Secretaria-Executiva.

Art. 4º O Comitê de Governança Estratégica reunir-se-á em caráter ordinário, preferencialmente, uma vez por mês, e, em caráter extraordinário, por convocação do Presidente ou do seu substituto.

§ 1º O quórum de reunião do Comitê de Governança Estratégica é de maioria simples de seus membros e o quórum de aprovação é de maioria absoluta.

§ 2º Além do voto ordinário, o Presidente do Comitê terá o voto de qualidade em caso de empate.

§ 3º O Comitê deliberará sobre eventuais revisões do planejamento estratégico e convocará reuniões específicas para tanto.

Art. 5º As reuniões cujos membros estejam em entes federativos diversos serão realizadas por videoconferência, salvo na hipótese de ser demonstrada, de modo fundamentado, a inviabilidade ou a inconveniência de realização nesse formato.

Art. 6º A participação no CGE será considerada serviço público relevante, não ensejando remuneração adicional para esta finalidade.

Art. 7º Os casos omissos serão dirimidos pelo Presidente do CGE.

ANEXO II

COMISSÃO TÉCNICA DO COMITÊ DE GOVERNANÇA ESTRATÉGICA

Art. 1º A Comissão Técnica do Comitê de Governança Estratégica - CT-CGE será constituída pelo:

I - Subsecretário de Planejamento e Orçamento, que a coordenará;

II - Coordenador-Geral de Gestão Estratégica e Inovação Institucional;

III - Coordenador-Geral de Orçamento e Finanças; e

IV - representantes, um titular e um suplente, a serem designados formalmente pelos órgãos específicos singulares e entidades vinculadas do Ministério.

Art. 2º A Comissão Técnica do Comitê de Governança Estratégica terá as seguintes atribuições:

I - prestar assessoria técnica ao Comitê de Governança Estratégica - CGE, no tocante à implementação das recomendações do Comitê Interministerial de Governança - CIG;

II - aprovar minutas de documentos padronizados para apresentação dos relatórios de acompanhamento de execução de políticas públicas pelas unidades finalísticas do Ministério;

III - apresentar ao CGE relatório consolidado sobre a gestão das políticas públicas;

IV - propor a adoção de manuais e guias com medidas que contribuam para a implementação dos princípios e diretrizes de governança pública;

V - elaborar minutas de resoluções necessárias para a implementação dos princípios e diretrizes de governança pública; e

VI - propor ao CGE a carteira de políticas públicas do Ministério, bem como a sua atualização.

Art. 3º A CT-CGE aprovará o seu regimento interno contendo as regras de funcionamento, por meio de resolução de seu coordenador, a ser publicada no Boletim de Serviço do MJSP.

Art. 4º O monitoramento da gestão de políticas públicas será realizado no âmbito da CT-CGE e será guiado pelo Anexo XI dessa Portaria.

Art. 5º A Comissão Técnica do Comitê de Governança Estratégica reunir-se-á por convocação do Coordenador ou do seu substituto.

§ 1º O quórum de reunião da CT-CGE é de maioria simples de seus membros e o quórum de aprovação é de maioria absoluta.

§ 2º Além do voto ordinário, o Coordenador da CT-CGE terá o voto de qualidade em caso de empate.

Art. 6º As reuniões cujos membros estejam em entes federativos diversos serão realizadas por videoconferência, salvo na hipótese de ser demonstrada, de modo fundamentado, a inviabilidade ou a inconveniência de realização nesse formato.

Art. 7º A participação na CT-CGE será considerada serviço público relevante, não ensejando remuneração adicional para esta finalidade.

Art. 8º Casos omissos e dúvidas surgidas na aplicação do presente Anexo II serão dirimidos pelo Subsecretário de Planejamento e Orçamento do Ministério.

Art. 9º A Secretaria-Executiva poderá estabelecer diretrizes para o planejamento e a operacionalização do disposto neste Anexo.

ANEXO III

COMITÊ DE GOVERNANÇA ADMINISTRATIVA

Art. 1º Compete ao Comitê de Governança Administrativa - CGA:

I - prestar assessoria técnica ao Comitê de Governança Estratégica - CGE no tocante à implementação das recomendações do Comitê Interministerial de Governança - CIG relacionadas à gestão administrativa;

II - propor políticas da gestão administrativa à Secretaria-Executiva, bem como implementar, acompanhar e avaliar suas ações;

III - propor diretrizes para a melhoria contínua nas práticas da gestão administrativa, com alinhamento às estratégias e metas institucionais, e submeter à aprovação do CGE;

IV - fomentar a parceria entre os órgãos e entidades vinculadas do Ministério para o desenvolvimento de ações referentes às compras compartilhadas, à capacitação, ao treinamento e ao desenvolvimento profissional, dentre outras temáticas da gestão administrativa; e

V - submeter à Secretaria-Executiva as deliberações concernentes às comissões técnicas do Comitê, em consonância com as políticas, objetivos, indicadores, metas e iniciativas institucionais estratégicas.

Parágrafo único. O CGA poderá editar resoluções para o desempenho de suas competências e para as deliberações do CGE, por meio de publicação no Boletim de Serviço do MJSP.

Art. 2º O CGA será composto pelos chefes de Gabinete ou por servidores que exerçam atribuições equivalentes no âmbito das seguintes unidades da estrutura organizacional do MJSP:

I - Gabinete do Ministro;

II - Assessoria Especial de Controle Interno;

III - Assessoria Especial de Assuntos Federativos e Parlamentares;

IV - Assessoria Especial de Assuntos Legislativos;

V - Assessoria Especial Internacional;

VI - Secretaria-Executiva;

VII - Consultoria Jurídica;

VIII - Ouvidoria-Geral;

IX - Órgãos específicos singulares; e

X - Fundação Nacional do Índio.

§ 1º A função de Secretaria-Executiva do Comitê será exercida pela Subsecretaria de Administração.

§ 2º O Subsecretário de Administração e o Subsecretário de Planejamento e Orçamento coordenarão os trabalhos do Comitê, a depender do tema.

§ 3º A Coordenação do CGA poderá convidar representantes de outros órgãos e de unidades da estrutura organizacional do Ministério, com vistas a colaborar com atividades técnicas e à internalização de diretrizes gerais.

Art. 3º O Comitê reunir-se-á, ordinariamente, uma vez por bimestre, ou por convocação extraordinária de seus coordenadores.

§ 1º As reuniões serão, preferencialmente, realizadas por meio de videoconferência.

§ 2º O quórum de reunião do Comitê é de maioria absoluta e o quórum de aprovação é de maioria simples.

§ 3º Na hipótese de empate, além do voto ordinário, os Coordenadores terão o voto de qualidade.

Art. 4º O Comitê poderá criar comissões técnicas para elaboração de políticas, diretrizes, planos, normas técnicas ou operacionais sobre os temas de sua atuação, que deverão obedecer às seguintes regras:

I - limitação a um máximo de sete integrantes em cada comissão;

II - limitação a um total de três comissões operando simultaneamente; e

III - caráter temporário, com duração não superior a um ano.

Art. 5º O Comitê poderá aprovar o regimento interno contendo as regras de funcionamento, por meio de resolução da Secretaria-Executiva deste Comitê, a ser publicada no Boletim de Serviço do MJSP.

Art. 6º A participação no Comitê será considerada serviço público relevante, não ensejando remuneração adicional para esta finalidade.

Art. 7º Casos omissos e dúvidas surgidas na aplicação do presente Anexo III serão dirimidas pelo Subsecretário de Administração e, em casos que permeiam a sua competência regimental, pelo Subsecretário de Planejamento e Orçamento.

Art. 8º A Secretaria-Executiva poderá estabelecer diretrizes para o planejamento e a operacionalização do disposto neste Anexo.

ANEXO IV

INSTÂNCIAS DE SUPERVISÃO DE GESTÃO DE RISCOS E CONTROLES INTERNOS

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Para assessorar o Comitê de Governança Estratégica - CGE nas atividades de gestão de riscos e controles internos, relativas à definição e à implementação de diretrizes, políticas, normas e procedimentos, são definidas as instâncias de supervisão de gestão de riscos e controles internos com as atribuições estabelecidas nos termos deste Anexo.

Art. 2º As instâncias de supervisão de gestão de riscos e controles internos têm como função precípua apoiar e dar suporte aos diversos níveis hierárquicos do Ministério na integração das atividades de gestão de riscos e controles internos nos processos e atividades organizacionais.

Art. 3º As instâncias de supervisão são compostas por:

I - Comitê de Gestão de Riscos e Controles Internos - CGRC;

II - Unidade de Gestão de Riscos e Controles Internos - UGRC; e

III - Gestor de Processos.

CAPÍTULO II

DA COMPOSIÇÃO

Art. 4º O CGRC é composto pela Assessoria Especial de Controle Interno e sua Coordenação-Geral de Integridade e Riscos e pela Subsecretaria de Planejamento e Orçamento e sua Coordenação-Geral de Gestão Estratégica e Inovação Institucional da Secretaria-Executiva.

Art. 5º A UGRC é composta, em cada órgão de assistência direta e imediata ao Ministro, nas entidades vinculadas e nos órgãos específicos singulares do Ministério, pela alta administração e por servidores indicados pela alta administração.

Parágrafo único. No caso da Secretaria-Executiva, a UGRC poderá ser composta pelo Secretário-Executivo Adjunto, em substituição ao dirigente máximo do órgão.

Art. 6º O Gestor de Processos corresponde a todo e qualquer responsável pela execução de um determinado processo de trabalho, inclusive sobre a gestão de riscos e controles internos.

CAPÍTULO III

DAS ATRIBUIÇÕES E RESPONSABILIDADES

Art. 7º Compete ao CGRC:

I - propor aprovação ao CGE de práticas, princípios de conduta e padrões de comportamento relacionados à gestão de risco e controle internos a serem observados pelos órgãos do Ministério;

II - submeter à aprovação do CGE a utilização de boas práticas de gestão de governança, de riscos e controles internos a serem observadas pelos órgãos do Ministério;

III - coordenar e assessorar os órgãos de assistência direta e imediata ao Ministro, os órgãos específicos singulares do Ministério e a Fundação Nacional do Índio na implementação das metodologias e dos instrumentos para gestão de riscos e controles internos;

IV - atuar como facilitador na integração dos agentes responsáveis pela gestão de riscos e controles internos e prestar assessoria técnica sobre regulamentos e padrões exigidos na condução das atividades correlatas;

V - estimular a adoção de práticas institucionais de responsabilização dos agentes públicos na prestação de contas e efetividade das informações;

VI - incentivar a integração dos agentes responsáveis pela gestão de riscos e controles internos;

VII - auxiliar no funcionamento das estruturas de gestão de riscos e controles internos nos processos de trabalho, observadas as estratégias aprovadas pelo CGE;

VIII - elaborar e propor ao CGE políticas, diretrizes, metodologias e mecanismos de comunicação e monitoramento para a gestão de riscos e controles internos;

IX - promover a capacitação e a disseminação da cultura nos assuntos de gestão de riscos e controles internos;

X - orientar e emitir recomendações sobre gestão de riscos e controles internos;

XI - propor método de priorização de processos e categorias de riscos para gestão de riscos e controles internos;

XII - propor limites de exposição a riscos e níveis de conformidade, bem como limites de alçada para exposição a riscos dos órgãos de assistência direta e imediata ao Ministro, dos órgãos específicos singulares do Ministério e da Fundação Nacional do Índio;

XIII - dar conhecimento ao CGE dos riscos que podem comprometer o alcance dos objetivos estratégicos e a prestação de serviços de interesse público;

XIV - avaliar e orientar sobre os resultados de medidas de aprimoramento destinadas à correção das deficiências identificadas na gestão de riscos e controles internos;

XV - reportar ao CGE informações sobre a gestão de riscos e controles internos para subsidiar a tomada de decisões e assegurar que estejam disponíveis em todos os níveis no âmbito do Ministério; e

XVI - praticar outros atos de natureza técnica e administrativa necessários ao exercício de responsabilidades previstas neste artigo.

Parágrafo único. O modelo de gestão de riscos será aplicado a partir dos processos priorizados no MJSP, conforme metodologia de priorização de processos estabelecida pela unidade organizacional do MJSP responsável pelo tema.

Art. 8º Compete à UGRC:

I - assegurar o cumprimento e propor aprimoramentos ao CGRC da política de gestão de riscos e controles internos;

II - assessorar a gestão de riscos e controles internos dos processos de trabalho priorizados no âmbito dos órgãos de assistência direta e imediata ao Ministro, dos órgãos específicos singulares do Ministério e das entidades vinculadas;

III - aprovar o plano de implementação de controles, acompanhar a implementação das ações, avaliar os resultados e monitorar os riscos ao longo do tempo;

IV - assegurar que as informações adequadas sobre a gestão de riscos e controles internos estejam disponíveis em todos os níveis no âmbito dos órgãos de assistência direta e imediata ao Ministro, dos órgãos específicos singulares do Ministério e das entidades vinculadas;

V - disseminar a cultura, bem como estimular e promover condições à capacitação nos assuntos de gestão de riscos e controles internos;

VI - estimular práticas e princípios de conduta e padrões de comportamento no âmbito de sua atuação e fomentar a inovação e a adoção de boas práticas de gestão de riscos e controles internos;

VII - assegurar o cumprimento das recomendações e orientações emitidas pelas instâncias de supervisão de gestão de riscos e controles internos;

VIII - proporcionar o cumprimento de práticas que institucionalizem a responsabilidade dos agentes públicos responsáveis pela gestão de risco na prestação de contas e efetividade das informações;

IX - promover a integração dos agentes responsáveis pela gestão de riscos e controles internos;

X - promover a implementação de metodologias e instrumentos para a gestão de riscos e controles internos; e

XI - praticar outros atos de natureza técnica e administrativa necessários ao exercício de responsabilidades previstas neste artigo.

Parágrafo único. As entidades vinculadas ao Ministério deverão manter metodologia de gestão de riscos aderentes aos dispositivos deste Anexo.

Art. 9º Compete ao Gestor de Processos:

I - cumprir e propor aprimoramentos à UGRC da política de gestão de riscos e controles internos;

II - gerenciar os riscos dos processos de trabalho e implementar mecanismos de controles internos, se necessário;

III - elaborar e submeter o plano de implementação de controles à aprovação da UGRC;

IV - implementar e gerenciar as ações do plano de implementação de controles, avaliar os resultados e monitorar os riscos ao longo do tempo;

V - gerar informações adequadas sobre riscos e controles internos e reportá-las à respectiva UGRC;

VI - disseminar preceitos de comportamento íntegro e de cultura de gestão de riscos e controles internos;

VII - observar a inovação e a adoção de boas práticas de gestão de riscos e controles internos;

VIII - cumprir as recomendações e observar as orientações emitidas pelas instâncias de supervisão de gestão de riscos e controles internos;

IX - adotar princípios de conduta e padrões de comportamento relacionados aos riscos e controles internos;

X - cumprir as práticas institucionalizadas na prestação de contas, transparência e efetividade das informações; e

XI - praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

Parágrafo único. As competências do gestor de processos descritas no caput são aplicáveis, quando couber, às entidades vinculadas.

Art. 10. O CGRC reunir-se-á a cada dois meses, ordinariamente, ou por convocação extraordinária do Chefe da Assessoria Especial de Controle Interno.

Art. 11. A participação no Comitê será considerada serviço público relevante, não ensejando remuneração adicional para esta finalidade.

Art. 12. Casos omissos e dúvidas surgidas na aplicação do presente Anexo IV serão dirimidos pelo Chefe da Assessoria Especial de Controle Interno.

ANEXO V

COMISSÃO EXECUTIVA DO PROGRAMA DE INTEGRIDADE DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Art. 1º Compete à Comissão Executiva do Programa de Integridade do MJSP - CEPI:

I - elaborar e propor diretrizes, metodologias e mecanismos de controle relacionados à integridade;

II - coordenar e assessorar a implementação de metodologias e instrumentos do Programa de integridade do Ministério;

III - propor objetivos estratégicos para o Programa;

IV - adotar e aprimorar as boas práticas em gestão de integridade;

V - atuar como facilitador na integração dos agentes responsáveis pela gestão de integridade;

VI - apoiar e orientar:

a) as ações de capacitação nas áreas de gestão de integridade;

b) a promoção da disseminação da cultura de gestão de integridade; e

c) a implementação de práticas e princípios de conduta e padrões de comportamento.

VII - coordenar a elaboração e a implementação do Programa;

VIII - exercer o monitoramento contínuo das ações estabelecidas no plano de integridade do Programa;

IX - apresentar e submeter à apreciação do Comitê de Governança Estratégica - CGE os resultados do grau de maturidade do Programa; e

X - praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

Art. 2º A CEPI será composta pelos seguintes membros:

I - Chefe da Assessoria Especial de Controle Interno, que a coordenará;

II - Presidente da Comissão de Ética do MJSP;

III - Corregedor-Geral;

IV - Ouvidor-Geral;

V - Subsecretário de Administração;

VI - Subsecretário de Planejamento e Orçamento;

VII - Diretor de Tecnologia da Informação e Comunicação; e

VIII - Agentes de Integridade das unidades finalísticas, exceto as entidades vinculadas.

§ 1º Funcionarão como suplentes das autoridades listadas no caput os respectivos substitutos.

§ 2º Os Agentes de Integridade referentes ao inciso VIII serão os respectivos chefes de gabinete das unidades finalísticas e seus substitutos.

§ 3º Os ocupantes dos cargos referentes aos incisos I, II, III e IV, ou similar, do Departamento Penitenciário Nacional, da Polícia Federal e da Polícia Rodoviária Federal deverão compor a CEPI.

§ 4º As entidades vinculadas ao Ministério poderão participar da Comissão Executiva do Programa de Integridade, na qualidade de membro convidado.

Art. 3º A CEPI reunir-se-á quadrimestralmente, por convocação de seu Coordenador, para avaliar os resultados dos trabalhos e, se necessário, revisar o Plano de Integridade do Programa.

Parágrafo único. As reuniões da Comissão serão realizadas com a presença mínima de cinco membros e o quórum de aprovação será de maioria simples dos membros presentes, atribuído ao seu Coordenador o voto de qualidade.

Art. 4º As reuniões cujos membros estejam em entes federativos diversos serão realizadas por videoconferência, salvo na hipótese de ser demonstrada, de modo fundamentado, a inviabilidade ou a inconveniência de realização nesse formato.

Art. 5º Caberá à Assessoria Especial de Controle Interno prestar o apoio administrativo à Comissão.

Art. 6º As atividades da CEPI serão exercidas sem prejuízo das demais responsabilidades dos seus integrantes.

Art. 7º O CGE poderá editar resoluções necessárias à realização do Programa.

Art. 8º A participação na CEPI será considerada prestação de serviço público relevante, não ensejando remuneração adicional para esta finalidade.

Art. 9º Casos omissos e dúvidas surgidas na aplicação do presente Anexo V serão dirimidas pelo Chefe da Assessoria Especial de Controle Interno.

ANEXO VI

COMITÊ DE GOVERNANÇA DE DADOS E SISTEMAS DE INFORMAÇÃO

CAPÍTULO I

DA COMPOSIÇÃO

Art. 1º O Comitê de Governança de Dados e Sistemas de Informação - CGDI do MJSP será composto por representantes, titular e suplente, das seguintes unidades:

I - Ouvidoria-Geral;

II - Assessoria Especial de Controle Interno;

III - Assessoria Especial de Assuntos Legislativos;

IV - Secretaria-Executiva:

a) Subsecretaria de Administração;

b) Subsecretaria de Planejamento e Orçamento; e

c) Diretoria de Tecnologia da Informação e Comunicação;

V - Consultoria Jurídica;

VI - Órgãos específicos singulares do Ministério; e

VII - Fundação Nacional do Índio.

§ 1º A coordenação do Comitê será exercida por servidor indicado pelo Ouvidor-Geral.

§ 2º Os representantes, titular e suplente, serão designados formalmente pelos órgãos constantes no caput deste artigo.

§ 3º Os membros do Comitê de Governança de Dados e Sistemas de Informação indicados, incluindo-se os suplentes, deverão possuir capacidade decisória para representar a unidade.

CAPÍTULO II

DAS COMPETÊNCIAS

Art. 2º Compete ao Comitê de Governança de Dados e Sistemas de Informação MJSP:

I - prestar assessoria técnica ao CGE no tocante à gestão, ao compartilhamento, à transparência e abertura de dados, às informações e sistemas de informação;

II - manter atualizada a PGDS-MJSP, encaminhando as propostas de aprimoramento ao CGE, para aprovação;

III - dirimir dúvidas e decidir sobre conflitos entre os integrantes do Sistema de Governança de Dados e Sistemas de Informação do MJSP, quando relacionados à gestão, ao compartilhamento, à transparência e abertura de dados, às informações e sistemas de informação;

IV - aprovar:

a) seu próprio regimento interno e suas atualizações;

b) o manual do agente de curadoria de bases de dados e Sistemas de Informação e suas atualizações; e

c) as solicitações para captação ou fornecimento de base de dados e informações, podendo delegar tal atribuição ao Comitê Executivo Permanente;

V - monitorar as solicitações de abertura de bases de dados prevista no art. 6º do Decreto nº 8.777, de 11 de maio de 2016;

VI - avaliar as solicitações de abertura de bases de dados, conforme critérios estabelecidos pelo Comitê, e encaminhar para aprovação pelo CGDSIC;

VII - avaliar as propostas de conteúdo e sugestões de alteração do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC e da Política de Segurança da Informação e Comunicação - POSIC submetidas à aprovação do CGDSIC e do CGE, a fim de resguardar o alinhamento com a política e o plano de ação de governança de dados e sistemas de informação, bem como a compatibilidade e adequação à política de segurança da informação e comunicações da Administração Pública Federal, e encaminhar para aprovação pelo CGDSIC;

VIII - determinar a realização de estudos e levantamentos necessários à aplicação e ao aprimoramento da PGDS;

IX - avaliar constantemente a qualidade, a tempestividade, a acurácia, a validade, a completude e a consistência das bases de dados no âmbito do MJSP;

X - resolver controvérsias acerca da validade de informações cadastrais e regras de prevalência entre registros administrativos conflitantes no âmbito do MJSP;

XI - emitir orientações e diretrizes para o compartilhamento de bases de dados entre as unidades do MJSP ou entre estas e os órgãos e entidades da Administração Pública dos três Poderes da União, Estados, Distrito Federal e Municípios, respeitando a legislação referente ao sigilo e à proteção de dados pessoais;

XII - propor políticas, estruturas e diretrizes para integração dos sistemas que compõem a plataforma operacional, conforme normativos e orientações do governo e melhores práticas;

XIII - emitir orientações e formular propostas para assegurar a sustentação econômico-financeira do compartilhamento de bases de dados, tabelas, consultas e sistemas entre unidades que compõem o MJSP e entre estes e os demais órgãos e entidades da Administração Pública dos três Poderes da União, Estados, Distrito Federal e Municípios;

XIV - aprovar anualmente o Plano de Ações da PGDS do MJSP e o Relatório Anual de Governança de Dados e Sistemas de Informação;

XV - acompanhar o Plano de Dados Abertos e submetê-lo ao CGDSIC para aprovação; e

XVI - designar o representante do MJSP em órgãos, colegiados ou eventos afetos à governança de dados e sistemas de informação.

Parágrafo único. As decisões do Comitê poderão ser submetidas ao CGE, em casos de conflitos não resolvidos no âmbito do Comitê de Governança de Dados e Sistemas de Informação ou em casos considerados estratégicos.

CAPÍTULO III

DISPOSIÇÕES FINAIS

Art. 3º O Comitê de Governança de Dados e Sistemas de Informação reunir-se-á:

I - anualmente, para priorizar o Plano de Ações da PGDS e apreciar e aprovar o Relatório Anual de Governança de Dados e Sistemas de Informação MJSP e o Relatório de Implementação do Plano de Dados Abertos; e

II - extraordinariamente, mediante convocação do coordenador.

Art. 4º O Comitê de Governança de Dados e Sistemas de Informação contará com uma Secretaria-Executiva, que será exercida pela Coordenação-Geral de Sistemas de Informação e Dados, da Diretoria de Tecnologia da Informação e Comunicação da Secretaria-Executiva, a qual auxiliará o coordenador na orientação, supervisão e execução das atividades do Comitê.

Art. 5º As decisões do Comitê de Governança de Dados e Sistemas de Informação serão tomadas por maioria simples dos votos dos membros, presente a maioria absoluta.

Art. 6º As reuniões do Comitê de Governança de Dados e Sistemas de Informação devem ser realizadas, preferencialmente, por videoconferência, quando houver participação de servidores lotados em localidade diversa da sede do MJSP.

Art. 7º O Comitê de Governança de Dados e Sistemas de Informação poderá instituir até três Comitês Executivos Técnicos, com duração máxima de um ano, para o desenvolvimento de estudos temáticos ou para execução de atividades decorrentes de suas deliberações, limitados a sete membros.

Art. 8º Poderão ser convidados para participar das reuniões do Comitê representantes de quaisquer órgãos ou entidades públicas ou privadas, bem como consultores técnicos especializados no assunto a ser tratado, sem direito a voto

Art. 9º A participação no Comitê será considerada serviço público relevante, não remunerada.

ANEXO VII

COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º O Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC é órgão de caráter consultivo e deliberativo, de atuação permanente, que tem por objetivo o estabelecimento de políticas e diretrizes sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação - TIC.

CAPÍTULO II

DAS COMPETÊNCIAS

Art. 2º Ao CGDSIC compete:

I - prestar assessoria técnica ao CGE no tocante aos assuntos relacionados à Tecnologia da Informação e Comunicação - TIC;

II - promover a integração entre as estratégias organizacionais e as estratégias da área de TIC;

III - estabelecer diretrizes de alinhamento entre soluções de TIC, a Estratégia de Governo Digital - EGD e o planejamento estratégico do Ministério;

IV - estabelecer as políticas de minimização de riscos, de priorização e distribuição dos recursos orçamentários de TIC;

V - aprovar o Plano de Transformação Digital do Ministério;

VI - aprovar o Plano de Dados Abertos do Ministério;

VII - aprovar e monitorar o Plano Estratégico de Tecnologia da Informação e Comunicação - PETIC;

VIII - Promover a elaboração, aprovar e monitorar a execução do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC, incluindo:

a) definição da abrangência e período de validade;

b) aprovação da composição do Grupo de Trabalho de elaboração;

c) priorização das necessidades de TIC; e

d) encaminhamento ao CGE para aprovação e ao Ministro para publicação.

IX - estabelecer e propor plano de investimento para a área de TIC;

X - definir prioridades na formulação e na execução de projetos relacionados à Tecnologia da Informação e Comunicação;

XI - aprovar, monitorar e manter a Política de Segurança da Informação e Comunicação - POSIC do Ministério e as normas internas de segurança da informação, observadas as disposições do art. 15, § 3º, do Decreto nº 9.637, de 26 de dezembro de 2018, e as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - orientar a criação e avaliar a Política de Governança de Tecnologia da Informação e Comunicação do Ministério por meio de um plano integrado de ações, considerando o planejamento estratégico do Ministério, as políticas e orientações do Governo Federal;

XIII - analisar os trabalhos e os pareceres técnicos afetos às suas competências que forem encaminhados pelos grupos de trabalho, pelas comissões e pela área de TIC do Ministério;

XIV - avaliar, periodicamente, o modelo e os mecanismos de governança de TIC, como estruturas, políticas e processos, verificando seu alinhamento estratégico e a efetividade dos mecanismos, em apoio ao CGE;

XV - avaliar o portfólio de TIC para garantir o alinhamento com os objetivos estratégicos do órgão, quanto a:

a) riscos;

b) conformidade com leis, regulamentos internos e externos, processos de negócio e demais boas práticas;

c) eficácia de desempenho e de resultados, durante e após os projetos; e

d) eficiência em termos de custo, sem redundância de investimentos e com viabilidade técnica para preservar o investimento no tempo;

XVI - propor diretrizes básicas ao CGE para a política de gestão de pessoas na área de TIC do Ministério;

XVII - propor estratégias e normas relacionadas à gestão dos recursos de TIC, zelando pelo seu cumprimento, cabendo ao CGE a sua aprovação, quando necessário;

XVIII - propor diretrizes relacionadas com a salvaguarda dos recursos de TIC ao CGE;

XIX - avaliar os fatores de riscos de TIC e averiguar se as decisões estratégicas estão sendo realizadas em conformidade com as avaliações, bem como com a política de riscos do Ministério;

XX - propor planos de comunicação e de resposta a riscos de TIC;

XXI - exercer as funções e atribuições de Comitê de Governança Digital de que trata a Estratégia de Governo Digital - EGD, deliberando sobre os assuntos relativos à implementação das ações de governo digital e ao uso de recursos de tecnologia da informação e comunicação; e

XXII - editar Resoluções para o desempenho de suas competências, por meio de publicação no Boletim de Serviço do MJSP.

CAPÍTULO III

DA COMPOSIÇÃO

Art. 3º O CGDSIC será composto por um titular e um suplente indicados no âmbito das seguintes unidades organizacionais, incluindo-se, dentre eles, o encarregado do tratamento de dados pessoais:

I - Ouvidoria-Geral;

II - Assessoria Especial de Controle Interno;

III - Secretaria-Executiva:

a) Subsecretaria de Administração;

b) Subsecretaria de Planejamento e Orçamento; e

c) Diretoria de Tecnologia da Informação e Comunicação;

IV - órgãos específicos singulares do Ministério, com exceção da Polícia Federal e da Polícia Rodoviária Federal; e

V - representante do Comitê de Governança de Dados e Sistemas de Informação.

§ 1º Os representantes serão indicados e designados em ato do Secretário-Executivo.

§ 2º À exceção do encarregado do tratamento de dados pessoais e do Comitê de Governança de Dados e Sistemas de Informação, os membros titulares do CGDSIC deverão ser ocupantes de cargos de Direção e Assessoramento Superiores ou Funções Comissionadas do Poder Executivo de nível 5 ou superior, e os suplentes, de nível 4 ou superior.

§ 3º O CGDSIC será presidido pela Diretoria de Tecnologia da Informação e Comunicação da Secretaria-Executiva, a qual exercerá o papel de Gestor de Segurança da Informação e Comunicação.

§ 4º Ao Gestor de Segurança da Informação e Comunicação compete, perante o CGDSIC:

I - coordenar a elaboração da Política de Segurança da Informação e Comunicação e das normas internas vinculadas, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

II - assessorar a alta administração na implementação da Política de Segurança da Informação e Comunicação;

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

IV - promover a divulgação da política e das normas internas de segurança da informação e comunicação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

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

VI - propor recursos necessários às ações de segurança da informação e comunicação;

VII - designar os integrantes da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR;

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

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

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação e comunicação; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação e comunicação.

CAPÍTULO IV

DISPOSIÇÕES FINAIS

Art. 4º O apoio administrativo ao CGDSIC caberá à Coordenação-Geral de Gestão de Governança de Tecnologia da Informação e Comunicação - CGGOV, sob supervisão do Diretor de Tecnologia da Informação e Comunicação.

Art. 5º O Presidente do CGDSIC poderá convidar representantes de outros órgãos e entidades, bem como consultores técnicos, com vistas a colaborar com atividades técnicas, sem direito a voto.

Art. 6º O CGDSIC poderá criar comissões técnicas e grupos de trabalho para auxiliar nas decisões do Comitê e para a elaboração de proposição de políticas, diretrizes, planos, normas técnicas ou operacionais sobre os temas de sua atuação, obedecidas as seguintes condições:

I - número máximo de sete membros, além de até dois representantes de cada unidade integrante do CGDSIC;

II- duração não superior a um ano; e

III - limite de até cinco subcolegiados operando simultaneamente.

Art. 7º O CGDSIC poderá se reunir a cada trinta dias, ordinariamente, ou por convocação extraordinária de seu Presidente.

§ 1º O quórum de reunião do Comitê é de maioria absoluta e o quórum de aprovação é de maioria simples.

§ 2º Na hipótese de empate, além do voto ordinário, o Presidente terá o voto de qualidade.

§ 3º As reuniões cujos membros estejam em entes federativos diversos serão realizadas por videoconferência, salvo na hipótese de ser demonstrada, de modo fundamentado, a inviabilidade ou a inconveniência de realização nesse formato.

Art. 8º A participação no Comitê será considerada serviço público relevante, não ensejando remuneração adicional para esta finalidade.

Art. 9º O CGDSIC aprovará seu regimento interno com suas regras de funcionamento, a ser publicado no Boletim de Serviço do MJSP.

Art. 10. Casos omissos e dúvidas surgidas na aplicação do presente Anexo VII serão dirimidos pelo Diretor de Tecnologia da Informação e Comunicação.

Art. 11. A Secretaria-Executiva poderá estabelecer diretrizes para o planejamento e a operacionalização do disposto neste Anexo.

ANEXO VIII

DA POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º A Política de Gestão de Riscos e Controles Internos - PGRCI será executada no âmbito do Ministério, com a finalidade de estabelecer princípios, diretrizes e responsabilidades mínimas a serem observados na execução dos planos estratégicos, programas, projetos e processos.

Art. 2º A PGRCI e suas eventuais normas complementares, metodologias, manuais e procedimentos aplicam-se aos órgãos de assistência direta e imediata ao Ministro, aos órgãos específicos singulares e colegiados do Ministério, abrangendo servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades no Ministério.

Parágrafo único. As entidades vinculadas poderão adotar práticas de gestão de riscos e de controle interno próprios, em observância às determinações e diretrizes constantes no Decreto 9.203, de 2007, e desde que alinhados com os princípios estabelecidos nos artigos 4º e 5º deste Anexo.

Art. 3º Para os efeitos deste Anexo VIII, entende-se por:

I - apetite a risco: nível de risco que o Ministério está disposto a aceitar;

II - atividade de controle interno: políticas e procedimentos adotados para mitigar os riscos que a organização tenha optado por tratar, de modo a assegurar que os objetivos sejam alcançados dentro dos padrões estabelecidos;

III - avaliação de risco: processo de análise quantitativa e qualitativa dos riscos relevantes que podem impactar o alcance dos objetivos do Ministério, com a indicação precisa da resposta apropriada, contemplando a identificação, avaliação e resposta ao risco;

IV - consequência: resultado de um evento que afeta positiva ou negativamente os objetivos do Ministério;

V - controle: qualquer medida aplicada no âmbito do Ministério para gerenciar os riscos e aumentar a probabilidade de que os objetivos e as metas estabelecidos sejam alcançados;

VI - controle interno da gestão: conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados, de forma integrada, pela direção e pelo corpo de servidores, destinados a enfrentar os riscos e fornecer segurança razoável para a consecução da missão do Ministério;

VII - fraude: qualquer ato ilegal caracterizado por desonestidade, dissimulação ou quebra de confiança, que não implique o uso de ameaça física ou moral;

VIII - identificação de riscos: processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais, podendo envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

IX - incerteza: incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros;

X - impacto: efeito resultante da ocorrência do evento;

XI - mensuração de risco: processo que visa estimar a importância de um risco e calcular a probabilidade de sua ocorrência;

XII - monitoramento: processo de observação sistemática, verificação e registro regular de uma atividade, de modo que as informações geradas constituam um elemento de tomada de decisão por parte do responsável pelo processo;

XIII - nível de risco: magnitude de um risco, expressa em termos da combinação de suas consequências e possibilidades de ocorrência;

XIV - operações econômicas: operações de aquisição de insumos necessários na quantidade e qualidade adequadas, sendo entregues no lugar certo e no momento preciso ao custo mais baixo;

XV - operações eficientes: operações nas quais é consumido o mínimo de recursos para alcançar uma dada quantidade e qualidade de resultados, ou ainda, alcançar o máximo de resultado com uma dada qualidade e quantidade de recursos empregados;

XVI - procedimentos de controle interno: procedimentos que o Ministério executa para enfrentar e tratar os riscos, projetados para lidar com o nível de incerteza previamente identificado com vistas ao alcance de seus objetivos;

XVII - processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;

XVIII - proprietário do risco: pessoa ou entidade com a responsabilidade e a autoridade para gerenciar o risco;

XIX - probabilidade: possibilidade de ocorrência de um evento;

XX - resposta ao risco: qualquer ação adotada para lidar com risco, podendo consistir em:

a) aceitar o risco por uma escolha consciente;

b) transferir ou compartilhar o risco a outra parte;

c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou

d) mitigar ou reduzir o risco, diminuindo sua probabilidade de ocorrência ou minimizando suas consequências;

XXI - risco: possibilidade de ocorrer um evento que venha a ter impacto no cumprimento dos objetivos, sendo medido em termos de impacto e de probabilidade;

XXII - riscos para a integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção;

XXIII - risco inerente: risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade dos riscos ou seu impacto;

XXIV - risco residual: risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

XXV - riscos de imagem ou reputação do órgão: eventos que podem comprometer a confiança da sociedade ou de parceiros, de clientes ou de fornecedores, em relação à capacidade do Ministério em cumprir sua missão institucional;

XXVI - riscos financeiros ou orçamentários: eventos que podem comprometer a capacidade do Ministério de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

XXVII - riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do Ministério;

XXVIII - riscos operacionais: eventos que podem comprometer as atividades do Ministério, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

XXIX - tolerância ao risco: nível de variação aceitável quanto à realização dos objetivos;

XXX - tratamento de riscos: processo de estipular uma resposta a risco;

XXXI - categoria de riscos: classificação dos tipos de riscos definidos pelo Ministério que podem afetar o alcance de seus objetivos, observadas as características de sua área de atuação e as particularidades do setor público;

XXXII - método de priorização de processos: classificação de processos estabelecida a partir de metodologia proposta pela unidade organizacional do MJSP responsável pelo tema no MJSP; e

XXXIII - plano de implementação de controles: documento elaborado pelo gestor para registrar e acompanhar a implementação de ações de tratamento a serem adotadas em resposta aos riscos avaliados.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 4º São princípios da Gestão de Riscos:

I - atuação de forma sistemática, estruturada e oportuna, subordinada ao interesse público;

II - estabelecimento de níveis adequados de exposição a riscos;

III - estabelecimento de procedimentos de controles internos proporcionais aos riscos, observada a relação custo-benefício;

IV - agregação de valor ao Ministério;

V - apoio à tomada de decisão e à elaboração do planejamento estratégico; e

VI - apoio à melhoria contínua dos processos organizacionais.

Art. 5º São princípios dos Controles Internos:

I - aderência à integridade e aos valores éticos;

II - supervisão do desenvolvimento e do desempenho dos controles internos da gestão pela alta administração;

III - coerência e harmonização da estrutura de competências e responsabilidades dos diversos níveis de gestão;

IV - compromisso da alta administração em atrair, desenvolver e reter pessoas com competências técnicas, em alinhamento com os objetivos do Ministério;

V - definição de responsáveis pelos diversos controles internos da gestão no âmbito do Ministério;

VI - definição de objetivos que possibilitem a eficaz gestão de riscos;

VII - mapeamento das vulnerabilidades que impactam os objetivos, de forma que sejam adequadamente identificados os riscos a serem geridos;

VIII - identificação e avaliação das mudanças internas e externas que possam afetar significativamente os controles internos da gestão;

IX - desenvolvimento e implementação de atividades de controle que contribuam para a obtenção de níveis aceitáveis de riscos;

X - adequado suporte de tecnologia da informação para apoiar a implementação dos controles internos da gestão;

XI - definição de políticas e normas que suportem as atividades de controles internos da gestão;

XII - utilização de informações relevantes e de qualidade para apoiar o funcionamento dos controles internos da gestão;

XIII - disseminação de informações necessárias ao fortalecimento da cultura e da valorização dos controles internos da gestão;

XIV - realização de avaliações periódicas para verificar a eficácia do funcionamento dos controles internos da gestão; e

XV - comunicação do resultado da avaliação dos controles internos da gestão aos responsáveis pela adoção de ações corretivas, incluindo a alta administração

CAPÍTULO III

DOS OBJETIVOS

Art. 6º São objetivos da Gestão de Riscos e Controles Internos:

I - dar suporte à missão, à continuidade e à sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos do Ministério;

II - sistematizar e suportar a gestão de riscos e controles internos pelas premissas da metodologia do Committee of Sponsoring Organizations of the Treadway Commission - COSO, da Norma Internacional ISO 31000 e de boas práticas;

III - atuar de forma dinâmica e formalizada por meio de instrumentos que possibilitem a obtenção de informações úteis à tomada de decisão para a consecução dos objetivos institucionais e para a gestão dos riscos dentro de padrões definidos pelas instâncias supervisoras;

IV - aferir o desempenho da gestão de riscos e controles internos mediante atividades contínuas de monitoramento de implementação de controles e avaliação dos resultados propostos, tendo como referência o desempenho do planejamento estratégico;

V - capacitar os agentes públicos que exercem cargo, função ou emprego no Ministério, em gestão de riscos e controles internos, de forma continuada, por meio de soluções educacionais, em todos os níveis;

VI - desenvolver e implementar atividades de controle da gestão que considerem a avaliação de mudanças, internas e externas, contribuindo para identificação e avaliação de vulnerabilidades que impactam os objetivos institucionais;

VII - salvaguardar e proteger bens, ativos e recursos públicos contra desperdícios, perda, mau uso, dano, utilização não autorizada ou apropriação indevida;

VIII - instituir controles, com base no modelo de gestão de riscos e controles internos, considerando a relação custo-benefício e a agregação de valor ao Ministério; e

IX - assegurar que as informações produzidas sejam íntegras e confiáveis à tomada de decisões, ao cumprimento das obrigações de transparência e à prestação de contas.

CAPÍTULO IV

DOS INSTRUMENTOS

Art. 7º São instrumentos da Gestão de Riscos e Controles Internos:

I - as instâncias de supervisão de gestão de riscos e controles internos;

II - a metodologia, a gestão de riscos e controles internos do Ministério deve ser estruturada com base no modelo do Committee of Sponsoring Organizations of the Treadway Commission - COSO, da Norma Internacional ISO 31000 e boas práticas, contemplando os seguintes componentes:

a) ambientes interno e externo;

b) fixação de objetivos;

c) identificação de eventos;

d) avaliação de riscos;

e) resposta a riscos;

f) atividades de controles internos, informação e comunicação; e

g) monitoramento;

III - as ferramentas dos controles internos;

IV - a capacitação continuada;

V - as normas, os manuais e os procedimentos formalmente definidos pelas instâncias de supervisão de gestão de riscos e controles internos; e

VI - a solução tecnológica.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Art. 8º A implementação desta política será realizada de forma gradual e continuada, com prazo de conclusão de cinquenta meses a contar da publicação desta Portaria.

Art. 9º O modelo de gestão de riscos e controles internos utilizar-se-á do método de priorização de processos estabelecido pela unidade organizacional do MJSP responsável pelo tema.

Art. 10. Os casos omissos ou as excepcionalidades serão solucionados pelo Chefe da Assessoria Especial de Controle Interno.

ANEXO IX

PROGRAMA DE INTEGRIDADE DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º O Programa de Integridade do MJSP será estruturado nas seguintes diretrizes:

I - comprometimento e apoio da alta administração;

II - existência de Comissão responsável pela implementação do Programa de Integridade;

III - análise, avaliação e gestão dos riscos associados à integridade; e

IV - monitoramento contínuo das ações estabelecidas no plano de integridade do Programa.

Art. 2º Para os efeitos do disposto neste Anexo IX, considera-se:

I - programa de integridade: conjunto estruturado de medidas institucionais voltadas para a prevenção, a detecção, a punição e a remediação de desvios éticos, fraudes e atos de corrupção, em apoio à boa governança;

II - fraude: quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança, que não implicam o uso de ameaça de violência ou de força física;

III - padrão de conduta ilibada: comportamento correto, honesto, idôneo, responsável, com confiança, respeito e transparência; e

IV - risco à integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

Parágrafo único. Os riscos à integridade podem ser causa, evento ou consequência de outros riscos, tais como financeiros, operacionais ou de imagem.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 3º São princípios da integridade:

I - padrões de conduta ilibada;

II - idoneidade moral;

III - observância dos valores institucionais;

IV - transparência;

V - confiabilidade;

VI - prestação de contas;

VII - ações coerentes com os preceitos legais e com o interesse público; e

VIII - garantia do devido processo legal e da ampla defesa pelas instâncias de apuração.

CAPÍTULO III

DOS OBJETIVOS

Art. 4º O Programa de Integridade do MJSP tem como objetivos:

I - promover a cultura ética e a integridade institucional, focadas nos valores e no respeito às leis e aos princípios da Administração Pública;

II - fortalecer a integridade institucional do Ministério, que deve ser promovida por decisões baseadas no autoconhecimento e diagnose de vulnerabilidades;

III - definir critérios para o provimento dos cargos Grupo-Direção e Assessoramento Superiores e das Funções Comissionadas do Poder Executivo do Ministério, a partir da identificação de perfis e capacitação adequadas;

IV - definir políticas específicas com orientação de padrões de comportamentos esperados dos agentes públicos no relacionamento com os cidadãos, o setor privado e os grupos de interesses;

V - dotar os mecanismos de preservação da integridade com critérios de identificação e punição dos responsáveis por possíveis desvios de conduta;

VI - promover o comprometimento da alta administração e o envolvimento de todo o corpo funcional do Ministério na manutenção de um adequado ambiente de integridade;

VII - definir políticas públicas adequadas, capazes de evitar fraudes e atos de corrupção;

VIII - orientar a interação entre os agentes públicos e privados, com foco nos serviços e relacionamentos com os cidadãos;

IX - promover a transparência de informações à sociedade;

X - primar pela excelência da gestão;

XI - promover a participação e o controle social nos mecanismos de comunicação com o público externo, com o objetivo de estimular o recebimento de insumos sobre a implementação de melhorias e a obtenção de informações sobre desvios de conduta a serem apurados; e

XII - capacitar continuamente os agentes públicos que exercem cargo, função ou emprego no Ministério, por meio de soluções educacionais, em todos os níveis, no tema de integridade.

CAPÍTULO IV

DOS INSTRUMENTOS DO PROGRAMA DE INTEGRIDADE

Art. 5º O Programa de Integridade do MJSP tem como instrumentos:

I - as instâncias de supervisão de gestão de riscos e controles internos;

II - o funcionamento dos controles internos;

III - os procedimentos de responsabilização;

IV - o canal de denúncias;

V - a capacitação continuada;

VI - a metodologia adequada; e

VII - a solução tecnológica.

CAPÍTULO V

DA IMPLEMENTAÇÃO DO PROGRAMA DE INTEGRIDADE

Art. 6º O Programa de Integridade do MJSP será implementado a partir das seguintes etapas:

I - criação da Comissão Executiva do Programa de Integridade do MJSP - CEPI, de que trata o Anexo V;

II - levantamento de situação das unidades, de mecanismos e de instrumentos de integridade;

III - mapeamento e avaliação dos riscos para a integridade e identificação de vulnerabilidades;

IV - definição de resposta aos riscos mapeados e estabelecimento de medidas de tratamento;

V - elaboração do plano de integridade do Programa;

VI - aprovação do plano de integridade do Programa pelo Comitê de Governança Estratégica - CGE; e

VII - implementação, monitoramento, avaliação dos resultados e revisão do plano de ação do programa de integridade.

§ 1º O plano de integridade é um documento que organiza, em um conjunto sistêmico, as principais medidas a serem implementadas ou desenvolvidas, a fim de prevenir, detectar e remediar os riscos para a integridade.

§ 2º O plano de integridade contemplará as seguintes atividades:

I - estabelecimento e disseminação dos valores institucionais e dos padrões de ética e de conduta;

II - implementação ou desenvolvimento dos instrumentos para o programa de integridade;

III - promoção de capacitações e palestras sobre integridade;

IV - implementação de práticas e princípios de conduta e padrões de comportamento;

V - disseminação do canal de denúncias, com garantia de privacidade do denunciante; e

VI - outros atos de natureza operacional que se fizerem necessários.

§ 3º A elaboração, o desenvolvimento e a implementação do plano de integridade caberá à CEPI.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 7º As entidades vinculadas do Ministério poderão implementar programas específicos de integridade, em observância às determinações e diretrizes constantes no Decreto 9.203, de 2007, e aderência aos normativos sobre o tema.

Art. 8º Os casos omissos ou as excepcionalidades serão solucionados pelo Presidente do CGE.

Art. 9º O CGE poderá editar resoluções necessárias à realização do Programa de Integridade do MJSP.

ANEXO X

DO PROCESSO DE GESTÃO ESTRATÉGICA

Art. 1º Gestão estratégica é o processo gerencial contínuo e sistemático que objetiva definir a direção a ser seguida pelo Ministério, visando otimizar sua relação com os ambientes interno e externo, por meio do alcance dos objetivos propostos.

Parágrafo único. O processo de gestão estratégica inclui as etapas de elaboração, de monitoramento, de avaliação e de revisão.

Art. 2º A gestão estratégica será conformada em conjunto de normas, documentos e sistemas.

§ 1º O planejamento estratégico do Ministério será elaborado e publicado até o dia 30 de novembro do primeiro ano do mandato presidencial e buscará alinhamento com o Plano Plurianual - PPA.

§ 2º O Ministro de Estado da Justiça e Segurança Pública, o Secretário-Executivo ou o Secretário-Executivo Adjunto priorizarão os objetivos, os indicadores, as metas e os projetos.

§ 3º Para fins deste Anexo, consideram-se:

I - objetivos: os desafios a que a organização se propõe para cumprir sua missão e alcançar sua visão de futuro no cumprimento do papel institucional que lhe é reservado;

II - indicadores: os elementos de medição do alcance dos objetivos definidos para análise da efetividade da estratégia;

III - metas: os resultados quantitativo ou qualitativo que a organização pretende alcançar em um prazo determinado, visando o atingimento de seus objetivos; e

IV - projetos: as iniciativas temporárias que estão diretamente associadas ao alcance dos objetivos.

§ 4º O planejamento estratégico do Ministério será aprovado pelo Ministro de Estado da Justiça e Segurança Pública.

§ 5º A alta administração dos órgãos de assistência direta e imediata ao Ministro de Estado da Justiça e Segurança Pública, dos órgãos específicos singulares do Ministério e das entidades vinculadas serão responsáveis pela consecução dos objetivos e das metas, pela realização dos projetos e pelo fornecimento das informações necessárias ao acompanhamento dos indicadores, podendo designar servidores para a realização dos atos necessários ao sucesso das iniciativas.

§ 6º Será dado tratamento administrativo adequado à gestão de projetos estratégicos e ao acompanhamento de indicadores estratégicos, conforme orientações a serem expedidas pela Secretaria-Executiva.

§ 7º Os recursos orçamentários, financeiros, de pessoal, de infraestrutura e de tecnologia de informação e comunicação deverão ser priorizados para a consecução das atividades abrangidas nos indicadores, metas e projetos estratégicos.

Art. 3º O planejamento estratégico, seus desdobramentos e resultados serão monitorados e avaliados periodicamente, no âmbito do Comitê de Governança Estratégica - CGE, com o intuito de acompanhar a implementação da estratégia, de identificar possíveis desvios e de implementar ações corretivas, visando o alcance dos objetivos estratégicos.

§ 1º A periodicidade do monitoramento será, preferencialmente, mensal.

§ 2º As informações necessárias ao detalhamento dos indicadores e dos projetos estratégicos e ao monitoramento são de responsabilidade dos órgãos de assistência direta e imediata ao Ministro de Estado da Justiça e Segurança Pública, dos órgãos específicos singulares do Ministério e das entidades vinculadas responsáveis pelo elemento estratégico.

§ 3º As informações relativas aos indicadores e aos projetos estratégicos serão registradas em sistema apropriado, com tempo suficiente para subsidiar as reuniões de monitoramento

§ 4º Será dada adequada publicidade aos dados referentes aos elementos estratégicos e ao monitoramento da execução do planejamento estratégico.

§ 5º As revisões do planejamento estratégico ocorrerão simultaneamente aos ciclos quadrimestrais correspondentes, por ocasião das Reuniões de Avaliação da Estratégia - RAE.

Art. 4º O planejamento estratégico poderá ser revisado caso haja mudanças de diretrizes.

Art. 5º Os órgãos de assistência direta e imediata ao Ministro de Estado da Justiça e Segurança Pública, os órgãos específicos singulares do Ministério e as entidades vinculadas poderão:

I - elaborar planejamento estratégico setorial, que deverá estar em consonância com o disposto neste Anexo X, a ser aprovado pelo dirigente de cada órgão; e

II - estabelecer ou alinhar os normativos internos sobre planejamento estratégico para dar cumprimento a este Anexo X.

Art. 6º São elementos estratégicos básicos:

I - missão;

II - visão;

III - atributos de valor para a sociedade;

IV - objetivos estratégicos;

V - indicadores e metas estratégicos; e

VI - projetos estratégicos.

Art. 7º Integram o planejamento estratégico do Ministério como documentos essenciais:

I - cadeia de valor;

II - mapa estratégico;

III - indicadores e metas estratégicos; e

IV - carteira de projetos estratégicos.

Parágrafo único. Os documentos essenciais serão publicados pela Secretaria- Executiva no Boletim de Serviço MJSP.

Art. 8º O planejamento estratégico será disponibilizado nas páginas eletrônicas do Ministério, na intranet e na internet.

Art. 9º Os casos omissos e as dúvidas suscitadas na aplicação do disposto neste Anexo serão dirimidos pelo Presidente do CGE.

ANEXO XI

PROCESSO DE GESTÃO DE POLÍTICAS PÚBLICAS

Art. 1º As atividades finalísticas do Ministério serão estruturadas em uma Carteira de Políticas Públicas, aprovada pelo CGE;

Art. 2º A Carteira de Políticas Públicas do Ministério será controlada pelo CGE, que avaliará a inclusão, a exclusão ou a modificação das políticas que a compõe.

§ 1º A responsabilidade pela gestão das políticas públicas é dos órgãos específicos singulares e das entidades vinculadas do MJSP, incumbido de sua concepção, execução e controle.

§ 2º A alocação de recursos orçamentários buscará observar o desempenho das políticas públicas.

Art. 3º As políticas públicas deverão ser compiladas em lista exaustiva, seguindo, quando possível, as orientações e as sugestões contidas nos guias e nos manuais aprovados pelo Comitê Interministerial de Governança - CIG.

§ 1º A Carteira de Políticas Públicas será publicada por meio de resolução do CGE.

§ 2º A carteira poderá ser alterada mediante deliberação do Presidente do CGE, a pedido das unidades finalísticas, a qualquer tempo, para as políticas a serem realizadas naquele exercício.

§ 3º É vedada a realização de transferências voluntárias ou obrigatórias de despesas finalísticas, sejam quais forem os instrumentos, como a abertura de programas na Plataforma +Brasil, a celebração do Termo de Execução Descentralizada - TED, a celebração de contrato em benefício de terceiros ou a publicação de editais de chamamento, sem a respectiva vinculação à política pública incluída na carteira de políticas públicas do Ministério.

§ 4º A carteira deverá contemplar as políticas a serem realizadas em razão de emendas parlamentares, inclusive as de execução obrigatórias.

Art. 4º O controle da carteira de políticas públicas será apoiado pela Comissão Técnica do Comitê de Governança Estratégica - CT-CGE, que produzirá informações e realizará encaminhamentos de modo a fundamentar as manifestações do CGE.

§ 1º As unidades finalísticas informarão à CT-CGE a instituição, a ampliação ou a extinção de políticas.

§ 2º Os órgãos específicos singulares do Ministério e as entidades vinculadas, responsáveis pela gestão de políticas públicas do Ministério deverão apresentar à CT-CGE relatórios de monitoramento das políticas públicas, conforme cronograma e parâmetros aprovados pela CT-CGE.

§ 3º Para fins de aplicação do disposto no caput, os relatórios deverão alinhar-se às informações pertinentes ao desempenho do Plano Plurianual - PPA e contemplar minimamente as seguintes informações:

I - indicadores de monitoramento de execução da política pública; e

II - avaliação dos resultados da política pública e proposição de medidas corretivas que reduzam falhas e promovam a eficiência.

§ 4º Fica a Subsecretaria de Planejamento e Orçamento da Secretaria-Executiva deste Ministério autorizada a atualizar a carteira de políticas públicas, por ato próprio, quanto às informações relativas ao plano plurianual, às ações orçamentárias, aos planos orçamentários, aos projetos e indicadores estratégicos, à base legal e em relação a erros e omissões.

ANEXO XII

DA POLÍTICA DE GOVERNANÇA DE DADOS E SISTEMAS DE INFORMAÇÃO DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Governança de Dados e de Sistemas de Informação, automatizados ou não automatizados, do Ministério da Justiça e Segurança Pública - PGDS-MJSP, que passa a integrar o SG-MJSP.

Seção I

Das Definições

Art. 2º Para os fins do disposto neste Anexo XII, considera-se:

I - dado: sequência de símbolos ou valores, representados em algum meio, produzidos como resultado de um processo natural ou artificial;

II - informação: conjunto de dados organizados de tal forma que tenham valor ou significado em algum contexto;

III - ativo de informação: patrimônio corporativo composto por dados obtidos, produzidos ou processados no desenvolvimento das ações e atividades do MJSP, incluindo as informações e conhecimentos deles derivados;

IV - dado público: qualquer dado gerado ou sob a guarda governamental que não tenha o seu acesso restrito por legislação específica;

V - dados abertos: dados públicos representados em meio digital ou físico, estruturados em formato aberto, processáveis por máquina, referenciados na rede mundial de computadores e disponibilizados sob licença aberta que permita sua livre utilização, consumo ou cruzamento;

VI - dados restritos: dados que, não sendo passíveis de classificação em grau de sigilo, por seu teor, utilização ou finalidade, demandem medidas especiais de proteção;

VII - metadado: informação que descreve características de determinado dado, explicando-o em certo contexto de uso;

VIII - captação de base de dados: processo de aquisição sistemática de bases de dados, tabelas, consultas e demais ativos de informação, a serem processadas no desenvolvimento de ações e atividades do MJSP e suas unidades vinculadas, independentemente do instrumento que formalize a aquisição;

IX - Plano de Dados Abertos: documento orientador para as ações de implementação e promoção de abertura de dados de cada órgão ou entidade da administração pública federal, obedecidos os padrões mínimos de qualidade, de forma a facilitar o entendimento e a reutilização das informações;

X - Base de Dados: repositório de dados e informações relacionados a determinado tema ou finalidade e estruturados de maneira a permitir a sua consulta, atualização e outros tipos de operação processados por meios informáticos;

XI - Dicionário de dados: compilação completa ou parcial dos metadados que contém categorização em ordem convencionada;

XII - Catálogo de Bases de Dados e Sistemas: lista descritiva de todas as bases de dados e sistemas de informação do MJSP, com suas respectivas unidades gestoras e agentes de curadoria, bem como descrição da atividade, processo de trabalho, serviço público ou política pública a que a base de dados ou sistema está associado;

XIII - Catálogo de Bases de Dados Abertos: lista descritiva de todas as bases de dados abertos do MJSP;

XIV - Catálogo de Captação e Fornecimento de Bases de Dados e Informações: lista de todos os acordos de cooperação e demais instrumentos que concretizem a captação ou o fornecimento de informações e bases de dados no âmbito do MJSP;

XV - Unidades Gestoras de Bases de Dados e Sistemas de Informação: unidade do MJSP que responde pela gestão das informações de uma base de dados, em decorrência de:

a) possuir interesse direto na utilização dos ativos de informação que compõem a base, para a execução de processos ou atividades da sua cadeia de valor; e

b) possuir, preferencialmente, competência legal, normativa ou regimental pelo principal processo de trabalho relacionado à base de dados, cujo resultado está diretamente vinculado ao propósito do uso dessas informações na instituição;

XVI - agente de curadoria: pessoa natural que tem responsabilidade pela guarda, garantia de consistência, segurança, privacidade, autorização de uso e acesso ao dado;

XVII - alívio de gestão de bases de dados e demais ativos de informação: processo de desobrigação de uma unidade do MJSP em relação à gestão de uma base de dados, que deverá ser desativada, caso não haja impedimentos, ou transferida para outra unidade;

XVIII - valor de referência para os dados: escalas, limites, unidades ou universo de variação dos dados;

XIX - Dados Mestres: dados de referência que representam conceitos fundamentais de negócio, comuns à maioria das áreas do MJSP, e cuja disponibilidade e qualidade são determinantes para mitigar relevante risco operacional, financeiro, legal ou reputacional;

XX - Sistemas de informação: elementos, automatizados ou não, que organizam, armazenam e disponibilizam acesso ao dado e à informação;

XXI - análise: aplicação de um processo ou método analítico;

XXII - usabilidade dos dados: indica se as informações estão em um formato utilizável; XXIII - precisão dos dados: indica se os dados estão com a granularidade suficiente;

XXIII - atualização dos dados: indica o tempo antes que as informações atualizadas estejam acessíveis; e

XXIV - acurácia dos dados: indica se a informação reflete o dado no mundo real.

Seção II

Dos Objetivos

Art. 3º São objetivos da Política de Governança de Dados e Sistemas de Informação do MJSP:

I - assegurar a preservação da intimidade e privacidade das pessoas naturais, nos termos da lei;

II - assegurar a proteção dos dados pessoais e a preservação do sigilo das pessoas jurídicas, nos termos da lei;

III - assegurar a manutenção e o constante aprimoramento dos requisitos de segurança da informação e comunicação, dados, sistemas de informação e comunicação sob responsabilidade ou coordenação do MJSP;

IV - garantir, em quantidade, qualidade e tempestividade os insumos de dados e informações necessários ao cumprimento da missão institucional do MJSP;

V - promover a integração e a articulação entre as unidades que compõem o MJSP e entre estas e os demais Poderes da União, Estados, Distrito Federal e Municípios, para execução de políticas públicas orientadas por dados; e

VI - aprimorar a transparência pública do MJSP e assegurar o acesso aos dados públicos existentes, em formato aberto, permitida sua livre utilização, consumo e cruzamento.

Parágrafo único. Essa política pode ser revista a qualquer tempo para atualizar seus termos em relação às constantes mudanças tecnológicas que afetam os dados, as informações e os sistemas de informação objeto de sua regulamentação.

Seção III

Dos Princípios

Art. 4º São princípios da Política de Governança de Dados e Sistemas de Informação do MJSP:

I - fomento ao desenvolvimento da cultura de transparência e da participação social;

II - alinhamento com as diretrizes de gestão e preservação de documentos e informações, visando à integridade, à confiabilidade, à auditabilidade, à interoperabilidade, à tempestividade, à disponibilidade, à qualidade, à acurácia, à validade, à completude, à consistência dos dados e, quando for o caso, a sua confidencialidade;

III - amplo compartilhamento de infraestrutura, sistemas de informação, bancos de dados e demais ativos de informação no âmbito do MJSP, respeitadas as restrições legais;

IV - promoção da transformação digital e estímulo ao uso de soluções digitais na gestão e prestação de serviços públicos no âmbito do MJSP;

V - racionalização e sustentabilidade econômico-financeira das soluções de tecnologia da informação e comunicação de dados e sistemas de informação;

VI - utilização de soluções em nuvem nos casos em que houver justificativa técnica detalhando os riscos, a segurança, a governança, os requisitos dos sistemas, a infraestrutura e os dados;

VII - respeito à privacidade, à inviolabilidade da intimidade, da honra e da imagem das pessoas e instituições, nos termos da lei;

VIII - adoção e aprimoramento dos requisitos de segurança da informação, comunicações, dados e sistemas de informação; e

IX - preservação do sigilo das atividades de inteligência e investigação, nos termos da lei.

Seção IV

Do Escopo

Art. 5º Estão abrangidas pela Política de Governança de Dados e Sistemas de Informação do MJSP:

I - todos os dados e informações produzidos, custodiados, mantidos ou recebidos no âmbito do Ministério, bem como suas análises;

II - os processos de captação, de geração, de armazenamento, de integração, de utilização, de compartilhamento, de divulgação, de retenção e descarte de dados e informações no âmbito do Ministério; e

III - os sistemas de informação, análise dos dados e aplicações desenvolvidos, adquiridos, instalados ou utilizados no âmbito do Ministério.

Seção V

Dos Documentos da Política de Governança de Dados e Sistemas de Informação

Art. 6º São documentos da Política de Governança de Dados e Sistemas de Informação do MJSP:

I - o Plano Diretor de Tecnologia da Informação e Comunicações - PDTIC;

II - o Plano de Dados Abertos;

III - o Catálogo de Bases de Dados e Sistemas;

IV - o Catálogo de Bases de Dados Abertos;

V - o Catálogo de Captação e Fornecimento de Bases de Dados e Informações;

VI - o Plano de Ações da Política de Governança de Dados e Sistemas de Informação do Ministério da Justiça e Segurança Pública;

VII - a Política de Segurança da Informação e Comunicação - POSIC;

VIII - o Relatório Anual de Governança de Dados e Sistemas de Informação;

IX - o Manual do Agente de Curadoria de Bases de Dados e Sistemas de Informação;

X - os Dicionários de bases de dados; e

XI - outros documentos relativos à Política de Governança de Dados e Sistemas de Informação, a exemplo de regimentos, resoluções, atas, modelos de instrumentos de cooperação, acordos técnicos e termos de sigilo.

Parágrafo único. Sempre que possível, os modelos de que trata o inciso XI deverão ser disponibilizados na rede interna do MJSP.

CAPÍTULO II

DO SISTEMA DE GOVERNANÇA DE DADOS E SISTEMAS DE INFORMAÇÃO DO MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

Seção I

Da Composição

Art. 7º O Sistema de Governança de Dados e Sistemas de Informação do Ministério da Justiça e Segurança Pública - SGDS-MJSP é caracterizado pelo conjunto de práticas gerenciais, mecanismos de liderança, estratégias e controles, instituídos com a finalidade de estabelecer o modelo de tomada e decisão nos assuntos relacionados à gestão, ao compartilhamento, à transparência e abertura de dados, às informações e sistemas de informação.

Art. 8º O SGDS-MJSP é composto pelo (a):

I - Comitê de Governança Estratégica - CGE, instância máxima do SG-MJSP;

II - Comitê de Governança de Dados e Sistemas de Informação do Ministério da Justiça e Segurança Pública - CGDI-MJSP;

III - Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC;

IV - Diretoria de Tecnologia da Informação e Comunicações - DTIC;

V - Unidades Gestoras de Bases de Dados e Sistemas de informação - UGDS;

VI - Agentes de Curadoria de Bases de dados e Sistemas de informação - ACDS;

VII - Ouvidoria-Geral;

VIII - Assessoria Especial de Controle Interno; e

IX - Autoridade de Monitoramento da Lei nº 12.527, de 2011.

Seção II

Das Unidades Gestoras de Bases de Dados e Sistemas de Informação

Art. 9º As unidades do MJSP deverão se declarar gestoras das bases de dados e sistemas de informação sob sua responsabilidade, mediante o registro no Catálogo de Bases de Dados e Sistemas de Informação do MJSP.

Art. 10. Compete ao dirigente máximo da unidade gestora de bases de dados e sistemas de informação:

I - nomear e dispensar os agentes de curadoria de bases de dados e sistemas de informação sob sua responsabilidade, em número e qualificação suficientes;

II - propor nova captação de bases de dados e demais ativos de informação;

III - autorizar a criação de bases de dados e disponibilizar a proposta do respectivo dicionário de dados;

IV - recomendar ao Comitê de Governança de Dados e Sistemas de Informação a desativação de captações de informações e de bases de dados sob sua gestão;

V - solicitar ao Comitê de Governança de Dados e Sistemas de Informação a alteração ou a transferência da gestão de base de dados ou sistema para outra unidade do Ministério da Justiça e Segurança Pública;

VI - assegurar a qualidade, a autenticidade, a integridade e a atualidade dos dados abertos, observado o disposto no Capítulo IV deste Anexo; e

VII - assegurar a participação da unidade na implementação do Plano de Dados Abertos, inclusive quanto à elaboração dos metadados das bases de dados.

§ 1º No caso de solicitação de desativação de uma base de dados, bem como de alívio ou de transferência de gestão, as obrigações da unidade gestora solicitante remanescerão até que ocorra a efetiva extinção ou transferência de responsabilidade.

§ 2º A unidade gestora solicitante deverá providenciar o encerramento das captações de informações relacionadas, quando possível.

Art. 11. São responsabilidades das Unidades Gestoras de Base de Dados e Sistemas de Informação, a ser desempenhadas pelos respectivos agentes de curadoria:

I - definir e manter atualizados:

a) as regras de retenção e de descarte das bases de dados, tabelas, consultas e sistemas de informação;

b) os valores de referência para os dados;

c) os requisitos, as regras de negócio e as métricas para a gestão da qualidade de dados, observadas as orientações do Comitê de Governança de Dados e Sistemas de Informação;

d) as regras de acesso às bases de dados, tabelas, consultas e sistemas de informação, conforme os respectivos critérios de segurança e classificação definidos pelo Comitê de Governança de Dados e Sistemas de Informação; e

e) os dicionários das bases de dados sob sua responsabilidade;

II - monitorar e controlar a qualidade, a tempestividade, a acurácia, a validade, a completude e a consistência dos dados;

III - identificar e promover a resolução de eventuais problemas nas informações;

IV - prover auxílio em relação ao acesso e à análise das informações;

V - assegurar o devido atendimento às consultas dos interessados, observadas as restrições cabíveis; e

VI - no caso de informações recebidas de outros órgãos e entidades:

a) propor ao Comitê de Governança de Dados e Sistemas de Informação documentos de dados e normativos para a criação e atualização de captações de bases de dados e informações;

b) manter atualizadas as informações constantes no Catálogo de Captação e Fornecimento de Bases de Dados e Informações;

c) monitorar as captações e fornecimentos de bases de dados, tabelas, consultas e informações, gerando os registros necessários à auditoria de observância; e

d) observar os procedimentos e adotar as medidas previstas no Regulamento de Auditoria de Observância;

VII - comunicar mudanças e problemas aos usuários das informações.

Art. 12. Se houver gestão compartilhada entre duas ou mais unidades do MJSP, deverá ser designado o gestor master, que será o representante das unidades gestoras junto às demais instâncias.

CAPÍTULO III

DA GOVERNANÇA DE BASES DE DADOS E SISTEMAS DE INFORMAÇÃO

Seção I

Da Captação e do Fornecimento de Bases de Dados e demais Ativos de Informação

Art. 13. Qualquer unidade do MJSP interessada em captar bases de dados e demais ativos de informação deverá formalizar o pedido ao Comitê de Governança de Dados e Sistemas de Informação.

§ 1º O pedido deve conter, quando for o caso:

I - justificativa para captação e respectivo fundamento legal;

II - manifestação da Consultoria Jurídica da unidade solicitante, quando o acesso envolver dados e informações restritos ou protegidos por sigilo;

III - destinatário do pedido;

IV - descrição mínima das bases de dados, tabelas, consultas ou informações que serão captadas, no padrão do Catálogo de Captação e Fornecimento de Bases de Dados e Informações do MJSP;

V - descrição da contrapartida, quando houver;

VI - estimativa dos custos da captação;

VII - minuta do Termo ou Acordo de Cooperação Técnica;

VIII - minuta do Plano de Trabalho;

IX - minuta do Termo de Acesso;

X - minuta do Termo de Responsabilidade e Manutenção de Sigilo;

XI - descrição do mecanismo tecnológico de compartilhamento;

XII - descrição do processo de trabalho, serviço público ou política pública que será beneficiada com a captação de bases de dado ou informação; e

XIII - identificação do gestor das bases de dados, tabelas, consultas ou informações.

§ 2º O pedido será formalizado no Sistema Eletrônico de Informações - SEI e deverá ser assinado pela autoridade máxima da unidade solicitante.

Art. 14. Recebido o pedido, o Comitê de Governança de Dados e Sistemas de Informação dará ciência da solicitação de captação a todas as unidades do Ministério da Justiça e Segurança Pública, que deverão formalizar, no prazo de dez dias, manifestação de interesse.

§ 1º A manifestação de interesse conterá a descrição do processo de trabalho, serviço público ou política pública que será beneficiada com a captação de bases de dados ou informações, bem como o fundamento legal da solicitação de acesso.

§ 2º A DTIC deverá atestar a viabilidade técnica dos mecanismos de captação de bases de dados e demais ativos de informação, observado o disposto no art. 15 deste Anexo.

§ 3º Definidas as unidades interessadas e a viabilidade técnica da captação de bases de dados e demais ativos de informação, o processo será devolvido à unidade solicitante para que confeccione os documentos necessários à concretização da captação, observando, quando couber, os modelos disponíveis na rede interna do Ministério da Justiça e Segurança Pública.

Art. 15. Respeitadas as restrições legais e os requisitos de segurança da informação e comunicação, a captação de bases de dados e demais insumos de informação no âmbito do MJSP deve aproveitar a todas as unidades do Ministério, sendo vedada mais de uma captação para o mesmo dado, base de dados, tabela ou consulta, salvo expressa autorização do Comitê de Governança de Dados e Sistemas de Informação.

Parágrafo único. Sem prejuízo do disposto no caput, os mecanismos de captação de bases de dados e demais ativos de informação serão desenvolvidos de forma a atender as necessidades de negócio de todas as unidades interessadas.

Art. 16. As solicitações para fornecimento de bases de dados e demais ativos de informação formalizadas por órgãos ou entidades não integrantes da estrutura do MJSP deverão ser encaminhadas à autoridade máxima da unidade gestora de base de dados e sistemas de informação, contendo, quando for o caso:

I - justificativa para captação e respectivo fundamento legal;

II - manifestação da Consultoria Jurídica da unidade solicitante, quando o acesso envolver dados e informações restritos ou protegidos por sigilo;

III - descrição do processo de trabalho, serviço público ou política pública que será beneficiada com a captação da base de dados e demais ativos de informação sob gestão MJSP;

IV - descrição mínima das bases de dados, tabelas, consultas ou informações que serão captadas, no padrão do Catálogo de Captação e Fornecimento de Bases de Dados e Informações do MJSP;

V - detalhamento do perfil dos servidores que terão acesso à base de dados e demais ativos de informação;

VI - descrição da contrapartida, quando houver;

VII - minuta do Termo ou Acordo de Cooperação Técnica;

VIII - minuta do Plano de Trabalho;

IX - minuta do Termo de Acesso;

X - minuta do Termo de Responsabilidade e Manutenção de Sigilo; e

XI - descrição do mecanismo tecnológico de compartilhamento.

§ 1º O pedido será formalizado no SEI e deverá ser assinado pela autoridade máxima da unidade solicitante.

§ 2º Quando a solicitação de fornecimento de bases de dados e demais ativos de informação não envolver, simultaneamente, possibilidade de captação de dados pelas unidades do MJSP, a unidade gestora de bases de dados e sistemas de informação deliberará acerca da sua aceitação, comunicando ao Comitê de Governança de Dados e Sistemas de Informação os fornecimentos autorizados e os respectivos destinatários.

§ 3º Os pedidos que envolverem captação de bases de dados pelas unidades do MJSP observarão o procedimento descrito nos artigos 13, 14 e 15 deste Anexo.

§ 4º A DTIC deverá atestar a viabilidade técnica dos mecanismos de fornecimento de bases de dados e demais ativos de informação.

Art. 17. A celebração de atos para captação ou compartilhamento de bases de dados e demais ativos de informação, observará as seguintes disposições:

I - quando a captação ou compartilhamento atender a apenas uma unidade do Ministério da Justiça e Segurança Pública, o acordo de cooperação técnica ou instrumento congênere deverá ser firmado pela autoridade máxima desta unidade;

II - quando a captação ou compartilhamento atender a mais de uma unidade do Ministério da Justiça e Segurança Pública, o acordo de cooperação técnica ou instrumento congênere deverá ser firmado pelas autoridades máximas de cada uma destas unidades; e

III - quando a captação ou compartilhamento ocorrer exclusivamente entre órgãos do Ministério da Justiça e Segurança Pública, fica dispensada a formalização por Acordo de Cooperação Técnica.

§ 1º Nos casos dos incisos I e II deste artigo, a celebração dos atos dependerá de autorização prévia e de aprovação do Comitê de Governança de Dados e Sistemas de Informação - CGDI.

§ 2º Nos casos do inciso III deste artigo, deverá ser elaborado ato conjunto simplificado estabelecendo responsabilidades, protocolos e informações técnicas, o qual deverá ser apresentado para ciência do Comitê de Governança de Dados e Sistemas de Informação - CGDI, que poderá expedir manifestação técnica caso verifique ser necessário.

§ 3º Em qualquer caso deverão ser observadas as normas de delegação de atribuições editadas no âmbito do Ministério da Justiça e Segurança Pública.

§ 4º Excepcionalmente, os atos previstos neste artigo poderão ser celebrados pelo Ministro de Estado da Justiça e Segurança Pública, pelo Secretário Executivo ou pelo Secretário Executivo-Adjunto, nos casos considerados estratégicos ou naqueles em que a autoridade signatária do ente, do órgão ou da entidade copartícipe for equivalente a estas autoridades, por exemplo, o Advogado-Geral da União, o Presidente do Banco Central, os Comandantes de Comandos Militares, os Presidentes do Supremo Tribunal Federal ou de Tribunais Superiores, o Procurador-Geral da República, os Presidentes do Conselho

Nacional de Justiça e do Conselho Nacional do Ministério Público, os Presidentes do Senado Federal e da Câmara dos Deputados, o Presidente do Tribunal de Contas da União, os Governadores dos Estados ou do Distrito Federal e autoridades de Estados estrangeiro ou organismos internacionais.

§ 5º A Secretaria-Executiva e o Gabinete do Ministro serão cientificados da celebração dos atos referidos neste artigo.

Art. 18. A gestão, a operacionalização, o controle e a avaliação de resultados dos acordos de cooperação técnica ou instrumentos congêneres e demais atos de captação ou compartilhamento de dados e demais ativos de informação serão de responsabilidade expressa das unidades do MJSP participantes e interessadas, inclusive nos atos especificados no § 4º do art. 17.

Seção II

Do Acesso a Sistemas

Art. 19. As solicitações de acesso a sistemas de informação desenvolvidos ou mantidos no âmbito do MJSP deverão ser encaminhadas à unidade gestora de bases de dados e sistemas de informação pela autoridade máxima da unidade ou do órgão solicitante, contendo:

I - justificativa para o acesso, com descrição detalhada do processo de trabalho, serviço público ou política pública associadas ao sistema acessado;

II - fundamentação legal para o acesso;

III - descrição do perfil dos servidores que terão perfil de acesso ao sistema e a finalidade do acesso; e

IV - termo de compromisso e manutenção de sigilo, quando for o caso.

§ 1º A solicitação será apreciada pela autoridade máxima da unidade gestora do sistema, no prazo máximo de dez dias.

§ 2º Os conflitos envolvendo acesso a sistemas de informação no âmbito do MJSP e unidades vinculadas serão submetidos ao Comitê de Governança de Dados e Sistemas de Informação.

§ 3º Havendo controvérsia acerca da possibilidade de acesso pela unidade ou pelo órgão solicitante, em razão do enquadramento da informação em hipótese legal de sigilo, a solicitação deverá ser encaminhada à Consultoria Jurídica do MJSP, a quem competirá dirimir a questão.

§ 4º Quando a solicitação for realizada por órgão externo ao MJSP e havendo manifestação da Consultoria Jurídica do órgão em sentido contrário à manifestação da Consultoria Jurídica deste Ministério, a controvérsia será dirimida pela Consultoria-Geral da União - CGU/AGU.

Seção III

Do Catálogo de Bases de Dados e Sistemas de Informação

Art. 20. Todas as bases de dados, tabelas, consultas e sistemas das unidades do MJSP devem estar declaradas no Catálogo de Bases de Dados e Sistemas de Informação.

§ 1º O Catálogo de Bases de Dados e Sistemas de Informação deverá conter:

I - descrição detalhada das tabelas do banco de dados;

II - descrição detalhada dos campos das tabelas do banco de dados;

III - descrição detalhada das relações entre as tabelas do banco de dados, no caso de banco de dados relacional;

IV - descrição detalhada dos itens de informação, no caso de bancos de dados não relacionais;

V - descrição do sigilo relativo à tabela, campo ou item de informação, com a respectiva fundamentação legal; e

VI - descrição detalhada do processo de trabalho, serviço público ou política pública as quais as bases de dados, sistemas ou demais itens de informação estão associados.

§ 2º As informações contidas no Catálogo de Bases de Dados e Sistemas de Informação serão categorizadas de acordo com a hipótese de sigilo ou restrição de acesso relativa a cada item de informação.

§ 3º As Bases de dados, as tabelas, as consultas ou os sistemas que não estiverem relacionados a pelo menos uma declaração no Catálogo de Bases de Dados e Sistemas de Informação devem ser encaminhados à desativação.

Seção IV

Do Catálogo de Captação e Fornecimento de Bases de Dados e Informações

Art. 21. Toda captação ou fornecimento de informações pelas unidades do MJSP devem estar declaradas no Catálogo de Captação e Fornecimento de Bases de Dados e Informações.

Parágrafo único. O Catálogo de Captação e Fornecimento de Bases de Dados e Informações deverá conter:

I - descrição detalhada das tabelas do banco de dados objeto de captação ou do fornecimento;

II - descrição detalhada dos campos das tabelas do banco de dados objeto de captação ou do fornecimento;

III - descrição detalhada das relações entre as tabelas do banco de dados, no caso de banco de dados relacional;

IV - descrição detalhada dos itens de informação, no caso de bancos de dados não relacionais;

V - descrição do sigilo relativo à tabela, ao campo ou ao item de informação, com a respectiva fundamentação legal;

VI - descrição da periodicidade de captação ou fornecimento e de atualização da base de dados e demais insumos de informação;

VII - descrição do órgão ou entidade fornecedor ou recebedor da base de dados ou demais insumos de informação;

VIII - descrição do mecanismo tecnológico de captação ou fornecimento da base de dados ou demais insumos de informação;

IX - descrição detalhada do custo para captação ou fornecimento da base de dados ou demais insumos de informação; e

X - descrição detalhada do processo de trabalho, do serviço público ou da política pública às quais as bases de dados ou demais insumos de informação estão associados.

CAPÍTULO IV

DA TRANSPARÊNCIA ATIVA E DO PLANO DE DADOS ABERTOS

Seção I

Da Transparência Ativa

Art. 22. A transparência ativa visa o aumento da disseminação de dados e informações para a sociedade, inclusive em formato aberto, de modo a incentivar a participação social e promover a melhoria da qualidade dos dados publicados.

Art. 23. A abertura de dados no MJSP será regida pelos seguintes princípios e diretrizes:

I - observância da publicidade das bases de dados como preceito geral e do sigilo como exceção;

II - garantia de acesso irrestrito às bases de dados, as quais devem ser legíveis por máquina e estar disponíveis em formato aberto, nos termos da legislação;

III - descrição das bases de dados, com informação suficiente para a compreensão de eventuais ressalvas quanto à sua qualidade e integridade;

IV - permissão irrestrita de reuso das bases de dados publicadas em formato aberto;

V - completude e interoperabilidade das bases de dados, as quais devem ser disponibilizadas em sua forma primária, com o maior grau de granularidade possível, ou referenciar as bases primárias, quando disponibilizadas de forma agregada;

VI - atualização periódica, de forma a garantir a perenidade dos dados, a padronização de estruturas de informação e o valor dos dados à sociedade e atender às necessidades de seus usuários;

VII - designação clara do responsável pela publicação, atualização, evolução e manutenção de cada base de dado aberta, incluída a prestação de assistência quanto ao uso de dados; e

VIII - a utilização de linguagem cidadã.

Art. 24. Os sistemas de informação desenvolvidos no âmbito do MJSP deverão, sempre que possível e compatível com suas finalidades, possibilitar a geração e a extração de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, bem como o acesso automatizado por sistemas de informação externos em formatos abertos, estruturados e legíveis por máquina.

Art. 25. As bases de dados a serem disponibilizadas em formato aberto devem ser priorizadas e justificadas em função de seu potencial em termos de interesse público.

Parágrafo único. Para garantir o grau de interesse público deverá ser adotado mecanismo de participação social.

Seção II

Do Plano de Dados Abertos

Art. 26. A priorização de bases de dados para elaboração do Plano de Dados Abertos observará os seguintes parâmetros:

I - o grau de relevância para o cidadão;

II - o estímulo ao controle social;

III - a obrigatoriedade legal ou o compromisso assumido de disponibilização daquele dado;

IV - o dado estar relacionado a projetos estratégicos do governo;

V - o dado deve demonstrar resultados diretos e efetivos dos serviços públicos disponibilizados ao cidadão pelo Estado;

VI - a sua capacidade de fomento ao desenvolvimento sustentável;

VII - a possibilidade de fomento a negócios na sociedade; e

VIII - os dados mais solicitados em transparência passiva desde o início da vigência da Lei nº 12.527, de 2011.

Art. 27. O Plano de Dados Abertos deverá conter, de forma obrigatória, os seguintes itens:

I - breve contextualização com o cenário institucional e os instrumentos de gestão;

II - objetivos gerais e específicos a serem atingidos;

III - relação de todas as bases de dados públicos contidas no inventário e catálogo corporativo do órgão ou entidade, devendo identificar:

a) as bases de dados já abertas e catalogadas no Portal Brasileiro de Dados Abertos;

b) as bases de dados já abertas e não catalogadas no Portal Brasileiro de Dados Abertos;

c) as bases de dados ainda não disponibilizadas em formato aberto na data de publicação do Plano de Dados Abertos; e

d) as políticas públicas às quais as bases estão relacionadas, quando aplicável;

IV - mecanismos transparentes de priorização na abertura de bases de dados, devendo constar explicitamente quais os mecanismos de consulta pública utilizados, data das consultas e local onde o conteúdo das sugestões da sociedade civil poderá ser acessado, em formato aberto;

V - descrição detalhada das estratégias adotadas pelo órgão ou pela entidade para viabilizar a execução da abertura dos dados em consonância com o cronograma de publicação; e

VI - plano de ação contendo cronograma:

a) de mecanismos para a promoção, o fomento, o uso e reuso efetivo das bases de dados pela sociedade e pelo Governo, contendo para cada ação prevista o nome e a descrição da ação, o mês e o ano de realização, a unidade de lotação, o nome e o contato do servidor e a área responsável pela ação no órgão ou na entidade; e

b) de publicação dos dados e recursos, contendo para cada base prevista o nome da base e o conjunto de dados, a descrição da base, o mês e o ano da publicação, os contatos das áreas temáticas responsáveis pela base no órgão ou na entidade e a periodicidade de atualização da base.

Art. 28. O Plano de Dados Abertos, aprovado pelo Ministro de Estado da Justiça e Segurança Pública, terá vigência de dois anos a contar da data de sua publicação.

§ 1º O Plano será publicado em transparência ativa, na seção "Acesso à Informação" e a Portaria que o aprovou deverá ser publicada na imprensa oficial.

§ 2º O Plano de Dados Abertos poderá ser revisado periodicamente para fins de monitoramento, acompanhamento e alinhamento estratégico com outros instrumentos de gestão do órgão, devendo o novo documento conter as motivações e justificativas para as modificações realizadas no documento original.

§ 3º As entidades vinculadas do Ministério elaborarão seus próprios Planos de Dados Abertos.

Art. 29. As bases de dados abertos serão catalogadas no Portal de Dados Abertos do MJSP a (http://dados.mj.gov.br/), devendo possuir a mesma nomenclatura utilizada no Plano de Dados Abertos.

Art. 30. Aos pedidos de abertura de base de dados de que trata o art. 6º do Decreto nº 8.777, de 11 de maio de 2016, aplicam-se os prazos e os procedimentos previstos para o processamento de pedidos de acesso à informação.

§1º As unidades deverão consultar a DTIC acerca da viabilidade técnica e do prazo necessário para eventual abertura da base de dados.

§ 2º O responsável pelo Serviço de Informação ao Cidadão - SIC deverá comunicar ao Comitê de Governança de Dados e Sistemas de Informação sobre os pedidos de abertura de bases de dados em até cinco dias.

§ 3º A unidade gestora da base, sempre que receber pedidos de abertura de bases por outros meios que não o SIC, deverá informar ao Comitê de Governança de Dados e Sistemas de Informação, em até cinco dias.

§ 4º O Comitê de Governança de Dados e Sistemas de Informação poderá solicitar o acompanhamento da análise do pedido de abertura de base dedados, conforme critérios por ele estabelecidos, ou poderá ser consultado pela unidade gestora da base objeto do pedido.

Art. 31. O Comitê de Governança de Dados e Sistemas de Informação poderá estabelecer regulamento complementar sobre os procedimentos para elaboração, implementação e monitoramento do Plano de Dados Abertos, as formas de publicação e atualização das bases de dados.

Seção III

Da Autoridade de Monitoramento da Lei de Acesso à Informação

Art. 32. São responsabilidades da Autoridade de Monitoramento da Lei nº 12.527, de 2011, no MJSP:

I - publicar e atualizar o Plano de Dados Abertos;

II - orientar as unidades sobre o cumprimento das normas referentes a dados abertos;

III - assegurar o cumprimento das normas relativas à publicação de dados abertos, de forma eficiente e adequada;

IV - monitorar a implementação dos Planos de Dados Abertos; e

V - apresentar relatórios periódicos sobre o cumprimento dos Planos de Dados Abertos, com recomendações sobre as medidas indispensáveis à implementação e ao aperfeiçoamento da Política de Dados Abertos.

Parágrafo único. Os relatórios de que trata o inciso V deverão ser publicados em transparência ativa, na seção "Acesso à Informação".

Seção IV

Da Ouvidoria-Geral

Art. 33. São responsabilidades da Ouvidoria-Geral:

I - zelar pela governança do Plano de Dados Abertos, por meio de monitoramento e acompanhamento de sua execução;

II - apoiar e fornecer suporte aos órgãos vinculados e unidades do MJSP para a disponibilização dos dados em formato aberto, subsidiando a publicação e a manutenção dos dados;

III - propor diretrizes, prazos e orientações técnicas ao Secretário-Executivo para o monitoramento, a avaliação, a gestão e a revisão do Plano Institucional de Dados Abertos;

IV - estimular a publicação das informações e sua catalogação no Portal Brasileiro de Dados Abertos, bem como a atualização das bases já catalogadas;

V - buscar a melhoria contínua da publicação de dados abertos junto aos órgãos e unidades detentores das informações publicadas; e

VI - realizar as providências necessárias para revisão e atualização periódica do Plano de Ação e a Matriz de Responsabilidades, conferindo-lhes ampla publicidade.

CAPÍTULO V

DA POLÍTICA DE CONFORMIDADE

Art. 34. Uma base de dados somente estará em conformidade com a PGDS-MJSP se:

I - houver unidade gestora e, pelo menos, um agente de curadoria designado;

II - estiver devidamente documentada no Catálogo de Bases de Dados e Sistemas de Informação;

III - mantiver referências íntegras aos dados mestres, quando for o caso; e

IV - estiver relacionada a sistema, atividade, processo de trabalho, serviço público ou política pública de competência do MJSP e suas unidades vinculadas.

Parágrafo único. A base de dados que não estiver em conformidade com a PGDS- MJSP deve ser encaminhada para desativação.

Art. 35. Um sistema de informação somente estará em conformidade com a PGDS- MJSP se:

I - houver descrição detalhada da sua utilidade e de suas funcionalidades;

II - houver descrição detalhada dos custos de manutenção no Catálogo de Bases de Dados e Sistemas de informação;

III - houver ato da unidade gestora detalhando eventuais perfis de acesso e características dos usuários; e

IV - houver ato da unidade gestora declarando a que atividade, processo de trabalho, serviço público ou política pública o sistema está relacionado.

Art. 36. A captação ou o fornecimento de bases de dados e demais insumos de informação somente estarão em conformidade com a PGDS-MJSP se:

I - estiver fundada em legislação pertinente;

II - estiver devidamente documentada no Catálogo de Captação e Fornecimento de Bases de Dados e Informações;

III - estiver relacionada a bases de dados declaradas no Catálogo de Bases de Dados e Informações; e

IV - estiver relacionada a sistema, atividade, processo de trabalho, serviço público ou política pública de competência do MJSP e suas unidades vinculadas.

Parágrafo único. A captação e o fornecimento de bases de dados e informações que não estiverem em conformidade com a PGDS-MJSP devem ser encaminhados para encerramento.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Art. 37. Dentro de cento e oitenta dias contados da data de publicação desta Portaria, as unidades organizacionais do MJSP deverão encaminhar ao Comitê de Governança de Dados e Sistemas de Informação a relação detalhada dos sistemas de informação, bases de dados, tabelas e consultas sob sua gestão, contendo:

I - descrição dos sistemas sob sua gestão e respectiva finalidade;

II - descrição detalhada dos bancos de dados e respectivas tabelas;

III - descrição detalhada dos campos das tabelas do banco de dados;

IV - descrição detalhada das relações entre as tabelas do banco de dados, no caso de banco de dados relacional;

V - descrição detalhada dos itens de informação, no caso de bancos de dados não relacionais;

VI - descrição do sigilo relativo à tabela, ao campo ou ao item de informação, com a respectiva fundamentação legal; e

VII - descrição detalhada do processo de trabalho, serviço público ou política pública as quais as bases de dados, os sistemas de informação ou os demais itens de informação estão associados.

Art. 38. Os acordos de cooperação, acertos, ajustes e demais instrumentos de captação de bases de dados e outros ativos de informação atualmente vigentes serão revistos no prazo de trezentos e sessenta dias contados da data de publicação desta Portaria, de forma a atender os objetivos, os princípios e as demais diretrizes aqui previstas.

ANEXO XIII

DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO - POSIC

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicação - POSIC, que passa a integrar o SG-MJSP.

CAPÍTULO II

DO ESCOPO

Art. 2º A Política de Segurança da Informação e Comunicação - POSIC tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, bem como orientar as atitudes adequadas no manuseio, no tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso contra ameaças e vulnerabilidades.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 3º As ações relacionadas com a segurança da informação e comunicação devem obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da ética, de auditoria e do não repúdio.

Parágrafo único. Devem ser adotadas como estratégias fundamentais de proteção:

I - privilégio mínimo: o acesso deve ser apenas às informações e recursos necessários para sua finalidade legítima;

II - defesa em profundidade: utilizar várias camadas de controle de segurança complementares;

III - elo mais fraco: a segurança total do sistema é igual à segurança oferecida pela sua proteção mais frágil; e

IV - simplicidade: quanto mais simples for um sistema, mais fácil é torná-lo seguro.

CAPÍTULO IV

DO ÂMBITO DE APLICAÇÃO

Art. 4º As disposições desta POSIC e eventuais normas complementares aplicam-se:

I - aos órgãos de assistência direta e imediata do Ministro;

II - aos órgãos específicos singulares e colegiados;

III - às entidades vinculadas do MJSP; e

IV - aos servidores, colaboradores, estagiários, consultores e quem, de alguma forma, desempenhe atividades no Ministério.

§ 1º É permitido aos órgãos de assistência direta e imediata ao Ministro, aos órgãos específicos singulares e colegiados, bem como às entidades vinculadas do Ministério que não integram o CGDSIC adotarem uma Política de Segurança da Informação e Comunicação própria.

§ 2º Os órgãos de assistência direta e imediata ao Ministro, os órgãos específicos singulares e colegiados, bem como as entidades vinculadas do Ministério que não integram o CGDSIC e que decidirem adotar a POSIC do MJSP deverão definir o seu modelo próprio de Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR e instituir sua criação.

Art. 5º As disposições desta POSIC também se aplicam, no que couber, ao relacionamento do Ministério com outros órgãos e entidades públicas ou privadas.

Parágrafo único. Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Ministério devem:

I - atender, no que couber, a essa política e demais normas relacionadas;

II - conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem; e

III - prever a obrigação de divulgação dessa política e suas normas complementares aos empregados envolvidos em atividades do contrato, por meio da assinatura de termo de ciência, quando a natureza de seu objeto ou condições específicas assim o exigirem.

CAPÍTULO V

DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os efeitos do disposto neste Anexo, adota-se a terminologia definida no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República por meio da Portaria GSI nº 93, de 26 de setembro de 2019, e revisões posteriores, considerando-se ainda as seguintes definições:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - alta administração: Ministros de Estado, ocupantes de cargos de natureza especial, ocupantes de cargo de nível 6 do Grupo Direção e Assessoramento Superiores - DAS ou Função Comissionada do Poder Executivo - FCP e presidentes e diretores de autarquias, inclusive as especiais, e de fundações públicas ou autoridades de hierarquia equivalente;

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

IV - ativo: qualquer coisa que tenha valor para a organização e para os seus negócios;

V - ativos de informação: um corpo de informações, definido e gerenciado como uma unidade única para que possa ser entendido, compartilhado, protegido e explorado de forma eficiente e cuja informação têm valor, risco, conteúdo e ciclos de vida reconhecíveis e gerenciáveis;

VI - 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 (em conformidade) à consecução dos objetivos;

VII - 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;

VIII - colaborador: pessoa jurídica ou pessoa física que desempenhe atividade de interesse do Ministério, realize estágio ou preste serviço, em caráter permanente ou eventual;

IX - computação em nuvem: modelo computacional que permite acesso por demanda e, independentemente da localização, a um 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;

X - 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;

XI - 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, que, via de regra, requer procedimentos de autenticação;

XII - custodiante: aquele que, de alguma forma, total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante ou dos ativos de informação que compõem o sistema de informação;

XIII - dados: informação processada ou armazenada por um computador podendo estar na forma de textos, documentos, imagens, áudios, clips, softwares, entre outros;

XIV - 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;

XV - dispositivos móveis: equipamentos portáteis dotados de capacidade computacional e dispositivos removíveis de memória para armazenamento, entre os quais se incluem notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos, cartões de memória, entre outros;

XVI - Equipe de Tratamento e Resposta a Incidentes Cibernéticos: grupo de pessoas com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, observando a política de segurança e os processos de gestão de riscos de segurança da informação e comunicação do órgão ou da entidade;

XVII - evento: qualquer mudança de estado que tenha significado para o gerenciamento de item de configuração ou serviço de TI;

XVIII - gestão de ativos de informação: atividade coordenada de uma organização para obter valor a partir dos ativos, o que envolve um equilíbrio entre custos, riscos e desempenho;

XIX - gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem, além de fornecer uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

XX - gestão de riscos de segurança da informação e comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;

XXI - gestão de segurança da informação e comunicação: 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 comunicação;

XXII - gestor de segurança da informação e comunicação: é responsável pelas ações de segurança da informação e comunicação no âmbito do órgão ou entidade da Administração Pública Federal;

XXIII - grau de sigilo: gradação de segurança atribuída a dados e informações em decorrência de sua natureza ou conteúdo;

XXIV - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXV - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

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

XXVII - não repúdio: garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá posteriormente negar sua autoria;

XXVIII - rede corporativa: sistema de transmissão de dados que transfere informações entre diversos equipamentos de uma mesma corporação e entre alguns desses equipamentos e o mundo externo;

XXIX - sistemas de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações em forma integrada;

XXX - Termo de Responsabilidade, Confidencialidade e Sigilo de Informação: 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;

XXXI - 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, Confidencialidade e Sigilo de Informação; e

XXXII - vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

CAPÍTULO VI

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 7º As ações de segurança da informação e comunicação deverão observar as disposições legais e regulamentares vigentes sobre o assunto.

CAPÍTULO VII

DAS DIRETRIZES GERAIS

Art. 8º A segurança da informação e comunicação é de responsabilidade de todos.

Art. 9º As ações de segurança da informação e comunicação devem considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, os requisitos legais, a estrutura e a finalidade do órgão.

Art. 10. As diretrizes de segurança da informação e comunicação descritas nesta Política devem ser observadas e cumpridas por todos os usuários que executem atividades vinculadas a este órgão durante todas as etapas do tratamento da informação, a saber:

I - produção;

II - recepção;

III - classificação;

IV - utilização;

V - acesso;

VI - reprodução;

VII - transporte;

VIII - transmissão;

IX - distribuição;

X - arquivamento;

XI - armazenamento;

XII - eliminação;

XIII - avaliação;

XIV - destinação; e

XV - controle da informação.

Art. 11. É condição para acesso aos ativos de informação do órgão a adesão formal aos termos desta política, mediante aceite de Termo de Responsabilidade, Confidencialidade e Sigilo de Informação.

Parágrafo único. A área de Tecnologia da Informação e Comunicação definirá o modelo do Termo de Responsabilidade, Confidencialidade e Sigilo de Informação a ser utilizado.

Art. 12. Todos os agentes públicos do órgão são responsáveis pela segurança dos ativos de informação e comunicação que estejam sob a sua responsabilidade e por todos os atos executados com sua identificação, tais como:

I - identificação de usuário da rede (Login);

II - crachá; e

III - endereço de correio eletrônico ou assinatura digital.

Art. 13. Os recursos de tecnologia da informação e comunicação disponibilizados pelo órgão devem ser utilizados dentro do seu propósito, observado o uso ético em conformidade com a legislação vigente.

Art. 14. Os contratos de prestação de serviços conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo, ainda, exigir da entidade contratada a assinatura de Termo de Responsabilidade, Confidencialidade e Sigilo de Informação quando a natureza de seu objeto ou condições específicas assim o exigirem.

Art. 15. As normas, os procedimentos, os manuais e as metodologias de segurança da informação e comunicação devem considerar, subsidiariamente, normas e padrões aceitos no mercado como referência nos processos de gestão e governança de segurança da informação e comunicação, e devem estipular mecanismos que objetivem a conformidade dos controles de segurança da informação e comunicação associados, inclusive a previsão de auditoria.

Art. 16. A integração e a sinergia entre as instâncias e estruturas de supervisão e apoio definidas nesta POSIC e aquelas definidas no sistema de governança do órgão devem ser asseguradas por meio de modelos de relacionamento que considerem e compartilhem, quando possível, as competências, responsabilidades, informações e as próprias estruturas.

CAPÍTULO VIII

DAS DIRETRIZES ESPECÍFICAS

Art. 17. Para cada uma das diretrizes constantes das seções deste Capítulo, deve ser avaliada a pertinência da elaboração de políticas, normas, procedimentos, orientações e/ou manuais complementares que disciplinem ou facilitem seu entendimento.

Seção I

Da Propriedade da Informação

Art. 18. As informações geradas, adquiridas ou custodiadas sob a responsabilidade do órgão são consideradas parte do seu patrimônio intelectual, não cabendo a seus criadores qualquer forma de propriedade, salvo aqueles direitos garantidos no âmbito da Lei nº 10.973, de 2 de dezembro de 2004, e em outras legislações, e devem ser protegidas segundo as diretrizes descritas nesta política, em seus documentos complementares e demais regulamentações em vigor.

Parágrafo único. Incluem-se como propriedade do órgão todos os dados produzidos por ferramentas de trabalho providas para o bom desempenho das atividades laborais, a exemplo de dados do correio eletrônico corporativo, dados compartilhados em ferramentas de colaboração institucionais, registros de uso da internet, dentre outros, respeitada a proteção dos dados pessoais, na forma da legislação vigente.

Seção II

Do Tratamento da informação

Art. 19. A informação custodiada que for manuseada, armazenada, transportada ou eliminada pelos agentes públicos deste órgão, no exercício de suas atividades, deve ser protegida segundo as diretrizes descritas nesta POSIC e nas demais regulamentações em vigor.

Art. 20. Toda informação criada, manuseada, armazenada, transportada ou eliminada pelo órgão deve ser avaliada e, quando cabível, classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada, conforme processo de classificação da informação implementado e mantido no órgão em conformidade com a legislação em vigor.

Art. 21. Toda informação criada, manuseada, armazenada, transportada, eliminada ou custodiada por este órgão é de sua responsabilidade e deve ser protegida adequadamente.

Seção III

Dos Controles de Acesso e do Acesso à Internet

Art. 22. Todos os eventos relevantes devem ser registrados para a segurança e o rastreamento de acesso às informações, conforme norma específica.

Parágrafo único. Devem ser criados mecanismos para assegurar a exatidão e a integridade dos registros de auditoria nos ativos de informação.

Art. 23. Todo agente público do órgão que utiliza os recursos de tecnologia da informação e comunicação deve ter uma conta de acesso própria, cuja concessão e revogação será regulamentada em norma específica.

§ 1º A identificação do usuário, por qualquer que seja o meio e a forma, deve ser pessoal e intransferível, permitindo o reconhecimento do usuário de maneira clara e irrefutável.

§ 2º O usuário é responsável por todos os atos praticados com o uso de sua identificação na rede de dados, no correio eletrônico, na utilização da assinatura digital e recursos criptográficos, dentre outros, ficando encarregado pela segurança dos ativos e processos que estejam sob sua responsabilidade.

§ 3º A autorização, o acesso, o uso da informação e dos recursos de tecnologia da informação e comunicação devem ser controlados e limitados ao que for necessário ao cumprimento das atribuições de cada agente público.

§ 4º Deve-se aplicar a segregação de funções para as atividades de controle de acesso, incluindo o pedido de acesso, a autorização de acesso e a administração de acesso.

Art. 24. O acesso à rede mundial de computadores - Internet, no ambiente de trabalho, será regulamentado em norma específica.

Seção IV

Da Gestão de Ativos

Art. 25. Os ativos associados à informação e aos recursos de processamento da informação devem ser identificados e associados a um proprietário e um inventário destes ativos deve ser estruturado e mantido, conforme norma específica.

§ 1º O uso aceitável das informações, dos ativos associados e dos recursos de processamento da informação deve ser identificado e documentado.

§ 2º Os ativos devem ser passíveis de monitoramento e ter seu uso investigado, quando necessário, por meio de mecanismos que permitam a rastreabilidade de seu uso.

Art. 26. O acesso dos usuários aos ativos de informação e sua utilização, quando autorizado, deve ser condicionado à assinatura do Termo de Responsabilidade, Confidencialidade e Sigilo de Informação, observando a legislação em vigor.

Seção V

Da Gestão de Riscos

Art. 27. As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação e comunicação, em conformidade com a Política de Gestão de Riscos e Controles Internos.

Parágrafo único. A gestão de riscos de tecnologia da informação deve avaliar os riscos relativos à segurança dos ativos de tecnologia da informação e a conformidade com exigências regulatórias ou legais.

Seção VI

Da Gestão da Continuidade do Negócio

Art. 28. A Estrutura de Segurança da Informação e Comunicação, em conjunto com as áreas responsáveis pelos ativos de informação, deverão instituir normas, procedimentos e controles que estabeleçam a gestão de continuidade do negócio, a fim de minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços.

§ 1º O plano de continuidade deve conter os requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre.

§ 2º Os controles de gestão de continuidade da segurança da informação estabelecidos e implementados devem ser verificados a intervalos regulares, para garantir que sejam válidos e eficazes em situações adversas.

Seção VII

Da Gestão de Incidentes de Rede

Art. 29. Os incidentes de segurança da informação devem ser identificados, monitorados, comunicados e devidamente tratados em tempo hábil, bem como registrados em relatório abrangendo desde sua identificação até o tratamento, de forma a possibilitar auditorias futuras pelas áreas responsáveis pelos respectivos ativos de informação impactados e garantir a continuidade das atividades.

Parágrafo único. As responsabilidades e procedimentos de gestão de incidentes de rede devem ser estabelecidos, respeitando-se a segregação de funções, para assegurar respostas rápidas, efetivas e ordenadas aos incidentes de segurança da informação.

Art. 30. A gestão de incidentes de segurança da informação será regulamentada por norma específica.

Seção VIII

Da Auditoria e Conformidade

Art. 31. O uso dos recursos de tecnologia da informação e comunicação disponibilizados por este órgão é passível de monitoramento e de auditoria, devendo ser implementados e mantidos mecanismos que permitam sua rastreabilidade.

§ 1º As atividades dos administradores e operadores do sistema devem ser registradas e os registros protegidos e analisados criticamente, a intervalos regulares.

§ 2º Os registros de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação devem ser produzidos, mantidos e analisados criticamente, a intervalos regulares.

Art. 32. Os controles de segurança da informação e comunicação devem ser analisados criticamente e verificados em períodos regulares pela Estrutura de Segurança da Informação e Comunicação, tendo por base a conformidade com políticas, padrões, normas, ferramentas, manuais de procedimentos e outros documentos pertinentes, de modo a assegurar que a segurança da informação esteja implementada e operada de acordo com as políticas e procedimentos da organização.

Art. 33. A privacidade, o sigilo e a proteção das informações de identificação ou de cunho pessoal devem ser asseguradas, observando a legislação vigente.

Seção IX

Do Uso e do E-mail

Art. 34. O serviço de correio eletrônico terá seu uso exclusivo por agentes públicos no exercício de suas funções.

Art. 35. As regras de acesso e utilização do e-mail corporativo deverão ser definidas por norma específica.

Seção X

Da Computação em Nuvem

Art. 36. Fica permitido o tratamento das informações em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de segurança da informação e comunicação.

§ 1º O tratamento das informações deve ser realizado em ambiente previamente homologado pela autoridade da área de Tecnologia da Informação e Comunicação.

§ 2º É vedado o tratamento, em ambiente de computação em nuvem, de informação classificada em grau de sigilo, conforme a legislação vigente.

Art. 37. Nas contratações de soluções de tecnologias da informação e comunicação que utilizem recursos de computação em nuvem, devem ser observados os regramentos e as legislações vigentes que tratam do armazenamento de dados, metadados, inclusive as cópias de segurança quanto à necessidade de permanência em território nacional.

Parágrafo único. A área de Tecnologia da Informação e Comunicação deve manter monitoramento visando garantir que o disposto no caput deste artigo seja cumprido.

Seção XI

Da Aquisição, do Desenvolvimento de Software Seguro e da Manutenção de Sistemas

Art. 38. A área de Tecnologia da Informação e Comunicação deve estabelecer critérios de segurança para o desenvolvimento, manutenção e aquisição de sistemas e aplicações.

§ 1º Os requisitos relacionados à segurança da informação devem ser incluídos nas especificações dos novos sistemas de informação ou melhorias dos sistemas de informação existentes.

§ 2º As metodologias e regras implantadas para o desenvolvimento de sistemas e software devem contemplar requisitos relacionados à segurança da informação e desenvolvimento seguro de software.

Seção XII

Dos Dispositivos Móveis

Art. 39. O uso dos dispositivos móveis portáteis providos aos agentes públicos deverá ser realizado exclusivamente no interesse do órgão.

Art. 40. Todo dispositivo móvel usado para acessar a rede corporativa estará submetido às normas de segurança da informação e comunicação estabelecidas.

Seção XIII

Da Segurança Física e do Ambiente

Art. 41. Deverão ser providos mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências, em resposta aos riscos.

Parágrafo único. Norma específica deverá ser editada para regulamentar o acesso a áreas seguras e proteção do perímetro.

Seção XIV

Da Segurança em Recursos Humanos

Art. 42. Os usuários devem ter ciência das ameaças e preocupações relativas à segurança da informação e comunicação e de suas responsabilidades e obrigações conforme estabelecidos nesta política.

Art. 43. Todos os usuários devem difundir e exigir o cumprimento desta política, de seus documentos complementares, das normas de segurança e da legislação vigente acerca do tema.

Art. 44. Todos os colaboradores do órgão e, quando pertinente, partes externas devem receber treinamento e atualizações regulares sobre as políticas e procedimentos organizacionais de segurança da informação e comunicação.

Art. 45. O gestor de Segurança da Informação e Comunicação disponibilizará canal de notificação, de forma anônima, para reportar violações dos procedimentos e políticas de segurança da informação, sendo dever dos usuários relatar qualquer desvio que possa comprometer a segurança da informação e comunicação.

Parágrafo único. Toda notificação deverá ser averiguada, registrada e tratada, devendo ser uma prática a divulgação desse canal no âmbito deste órgão.

Seção XV

Da Gestão de Operação e Comunicações

Art. 46. A área de Tecnologia da Informação e Comunicação deve estabelecer modelos e arquiteturas de referência que descrevam requisitos mínimos para a disponibilização de serviços, sistemas e infraestrutura, atendendo às necessidades operacionais e de segurança desta política.

Parágrafo único. Os procedimentos de operação devem ser documentados e disponibilizados para todos os usuários que deles necessitem.

Art. 47. A utilização dos recursos deve ser monitorada e ajustada e projeções devem ser feitas para necessidade de capacitação futura que garanta o desempenho necessário do sistema.

CAPÍTULO IX

DAS PENALIDADES

Art. 48. A não observância desta política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicação, acarretará, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Parágrafo único. A área de Tecnologia da Informação e Comunicação poderá adotar as providências emergenciais necessárias para cessar as ameaças à segurança da informação e comunicação.

CAPÍTULO X

DA ESTRUTURA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO E SUAS RESPONSABILIDADES

Art. 49. A segurança da informação e comunicação é disciplina fundamental da boa governança corporativa.

Art. 50. Fica instituída a Estrutura de Segurança da Informação e Comunicação com atribuições definidas nesta POSIC.

Art. 51. A Estrutura de Segurança da Informação e Comunicação deverá institucionalizar um modelo de gestão de segurança da informação e comunicação capaz de apoiar os diversos níveis hierárquicos do órgão com o objetivo de integrar os controles e processos de segurança da informação e comunicação aos processos organizacionais existentes.

Parágrafo único. A participação na referida estrutura e eventuais grupos de trabalho associados não enseja remuneração de qualquer espécie ou quaisquer criações de cargos além daqueles já existentes na estrutura regimental, sendo considerada serviço público relevante.

Art. 52. Em conformidade com a política de governança institucional, a Estrutura de Segurança da Informação e Comunicação é constituída por:

I - Comitê de Governança Estratégica - CGE;

II - Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC;

III - Gestor de Segurança da Informação e Comunicação;

IV - Comissão Permanente de Avaliação de Documentos - CPAD;

V - Comissão Permanente de Avaliação de Documentos Sigilosos - CPADS; e

VI - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

Parágrafo único. Os responsáveis por presidir ou coordenar as instâncias que formam a referida Estrutura de Segurança da Informação e Comunicação deverão garantir, em consonância com suas atribuições específicas, o cumprimento do disposto no Capítulo VII deste Anexo e o efetivo desempenho das competências da respectiva instância.

Art. 53. O CGE é a instância colegiada constituída como último nível para discussão de questões relativas à segurança da informação e comunicação, com caráter deliberativo.

Art. 54. O CGDSIC é unidade de apoio do CGE para temas relacionados com gestão de segurança da informação e comunicação, dentre outros.

Art. 55. A CPAD tem a responsabilidade de, dentre outros, orientar e realizar o processo de análise, avaliação e seleção da documentação produzida e acumulada no seu âmbito de atuação, tendo em vista a identificação dos documentos para guarda permanente e a eliminação dos destituídos de valor.

Art. 56. A CPADS tem a atribuição de opinar sobre a informação produzida no âmbito de sua atuação para fins de classificação em qualquer grau de sigilo, dentre outras.

Art. 57. A função de Gestor de Segurança da Informação e Comunicação é instituída pelo SG-MJSP.

Art. 58. A Estrutura de Segurança da Informação e Comunicação do Ministério deverá estipular e implementar mecanismos que apoiam e garantam o comprometimento dos recursos humanos na implementação das diretrizes desta POSIC.

Seção I

Da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR

Art. 59. Fica criada a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

§ 1º Compete ao Gestor de Segurança da Informação e Comunicação designar os integrantes da ETIR, suas atribuições, os serviços a serem prestados, modelo de implementação, público-alvo, autonomia, estrutura organizacional, escopo de atuação e demais exigências relacionadas ao desempenho de suas atividades, em cumprimento às disposições sobre a criação e o funcionamento de colegiados da administração pública federal.

§ 2º A Equipe de Tratamento e Resposta a Incidentes Cibernéticos será composta, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe.

§ 3º A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos.

§ 4º O Gestor de Segurança da Informação e Comunicação deverá instituir, no âmbito da área de Tecnologia da Informação e Comunicação, áreas de monitoramento, prevenção, reação, análise e inteligência de SIC, dentre outras, visando prestar apoio à ETIR.

Art. 60. A ETIR tem por missão identificar, receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança da informação e comunicação em sistemas computacionais, atuando também de forma proativa, com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer a missão da instituição, em consonância com as atividades de resposta e tratamento a incidentes em redes, tais como recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais.

CAPÍTULO XI

DAS DISPOSIÇÕES FINAIS

Art. 61. A POSIC e os documentos dela derivados deverão ser revisados sempre que mudanças significativas na estrutura do órgão ocorrerem ou quando alterações em normas e outras políticas forem aprovadas, ou ainda periodicamente a cada três anos, conforme a legislação vigente.

Art. 62. A POSIC e as normas e os procedimentos de segurança da informação e comunicação a ela associados deverão ser amplamente divulgados a todos que atuem direta e indiretamente no Ministério.