MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
Gabinete do Ministro

PORTARIA Nº 853, DE 5 DE SETEMBRO DE 2013

Aprova a Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI).

O MINISTRO DE ESTADO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO, no uso de suas atribuições e considerando o disposto no art. 5º da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, resolve:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI).

CAPÍTULO I

DO ESCOPO

Seção I

DO OBJETIVO

Art. 2º A Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI) alinha-se às estratégias do Ministério e objetiva garantir a disponibilidade, integridade, confidencialidade e autenticidade (DICA) das informações produzidas ou custodiadas pelo Ministério independentemente do meio onde estejam registradas.

Art. 3º A Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI) define as diretrizes, competências e responsabilidades relativas ao uso e compartilhamento de dados, informações e documentos em conformidade com a Legislação vigente, as normas técnicas pertinentes, os valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 4º Integram também a Posic/MCTI, os documentos que a complementam, destinados à proteção da informação e à disciplina de sua utilização.

Seção II

DA ABRANGÊNCIA

Art. 5º A Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI) aplica-se aos órgãos de assistência direta e imediata ao Ministro de Estado; aos órgãos específicos singulares e às unidades descentralizadas do Ministério e deve ser observada em todos os ambientes informatizados e/ou convencionais aqui elencados, devendo ser seguida por todos que, de alguma forma, executem atividades vinculadas a este Ministério.

Parágrafo único. Todos são responsáveis e devem estar comprometidos com a segurança da informação e comunicações do Ministério.

Art. 6º Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo Ministério devem atender a esta Política.

Art. 7º Esta Política também se aplica, no que couber, ao relacionamento do Ministério com outros órgãos e entidades públicos ou privados.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 8º Para efeitos desta Portaria entende-se por:

I. acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade. (Ref.: NC07/IN01/DSIC/GSIPR/2010);

II. agente público: todo aquele que exerce cargo, emprego ou função no Ministério da Ciência, Tecnologia e Inovação, ainda que transitoriamente com ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745/1993 e empregados públicos regidos pela Lei nº 9.962/2000, e colaboradores);

III. algoritmo de Estado: função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável (Ref.: NC09/IN01/DSIC/GSIPR/2013);

IV. ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (Ref.: NC04/IN01/DSIC/GSIPR/2013);

V. assinatura eletrônica: geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados por um indivíduo para ser um laço legalmente equivalente à assinatura manual do indivíduo;

VI. ativo classificado: ativo de informação com informação classificada;

VII. ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VIII. ativo sob restrição de acesso: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito;

IX. auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

X. auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões;

XI. autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema (Ref.: Lei nº 12.527/2011);

XII. colaborador: pessoa jurídica ou pessoa física que desempenhe atividade de interesse do MCTI, realize estágio ou preste serviço, em caráter permanente ou eventual;

XIII. Comitê de Segurança da Informação e Comunicações - CSIC: comitê instituído no âmbito dos órgãos de assistência direta e imediata ao Ministro de Estado, dos órgãos específicos singulares e das unidades descentralizadas do MCTI, por meio da Portaria MCTI nº

384, de 30 de maio de 2012, com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do Ministério;

XIV. confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

XV. continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido. (Ref.: NC06/IN01/DSIC/GSIPR/2009);

XVI. custodiante do ativo de informação: aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

XVII. desastres: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação (Ref.: NC06/IN01/DSIC/GSIPR/2009);

XVIII. disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados (Ref.: Lei nº 12.527/2011);

XIX. documento: unidade de registro de informações, qualquer que seja o suporte ou formato (Ref.: Lei nº 12.527/2011);

XX. documento classificado: documento com informação classificada;

XXI. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. (Ref.: NC03/IN01/DSIC/GSIPR/2009);

XXII. Gestão da Segurança da Informação e Comunicações: 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 comunicações. (Ref.: IN GSI/PR 01/2008).

XXIII. Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito do MCTI;

XXIV. Gestor do Ativo de Informação: autoridade legal responsável pela concessão de acesso a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo);

XXV. informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato (Ref.: Lei nº 12.527/2011);

XXVI. informações institucionais públicas: informações geradas ou custodiadas pelo MCTI ou por seus colaboradores, no exercício de suas funções, às quais o acesso será permitido, observando-se eventual restrição temporária. Dividem-se em:

a. de acesso ostensivo: aquelas que não estão sujeitas a nenhuma restrição de acesso;

b. de acesso transitoriamente restrito: aquelas referentes a documentos utilizados como fundamento de decisões e atos administrativos, às quais o acesso será franqueado após a edição do correspondente ato decisório, conforme previsto no parágrafo 3º do art. 7º da LAI, salvo se forem, posteriormente, objeto de classificação como sigilosas.

XXVII. informações institucionais não públicas: informações geradas ou custodiadas pelo MCTI ou por seus colaboradores, no exercício de suas funções, sujeitas a restrição de acesso. Dividem-se em:

a. informações pessoais: aquelas relacionadas à pessoa natural identificada ou identificável e que diga respeito à sua intimidade, vida privada, honra e imagem, cujo tratamento é regulado pelo art. 31 da LAI;

b. informações sujeitas a outros tipos de sigilo: aquelas sob segredo de justiça ou protegidas por sigilo comercial, bancário, fiscal, industrial ou outros, na forma da legislação vigente, conforme o disposto no art. 22 da LAI;

c. informação classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada;

d. registros: informações contidas em anotações, levantamentos e análises preliminares, ou sejam aquelas de produção e guarda dos agentes públicos no exercício de suas funções, e que não integrem processo ou expediente que subsidie decisão administrativa editada.

XXVIII. informação sob restrição de acesso: informação institucional não pública ou informação de acesso transitoriamente restrito;

XXIX. integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino (Ref.: Lei nº 12.527/2011);

XXX. legalidade: atributo que garante a legalidade jurídica da informação, assegurando que todos os seus dados estão de acordo com as cláusulas contratuais pactuadas ou com a legislação nacional ou internacional vigente;

XXXI. não repúdio: propriedade da informação que não possa ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;

XXXII. Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações (Ref.: IN GSI/PR 01/2008);

XXXIII. princípios: são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;

XXXIV. privacidade: propriedade da informação privada que só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata;

XXXV. quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações (Ref.: IN GSI/PR 01/2008);

XXXVI. recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração (Ref.: IN GSI/PR 03/2013);

XXXVII. recursos de tecnologia da informação: servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de Tecnologia da Informação;

XXXVIII. segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Ref.: IN GSI/PR 01/2008);

XXXIX. tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação (Ref.: Lei nº 12.527/2011);

XL. usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do MCTI mediante autorização de gestores de ativos;

XLI. vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação (Ref.: NC04/IN01/DSIC/GSIPR/2013).

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 9º Esta Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI) observa a legislação e normas específicas destacando-se:

I. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

II. Lei nº 8.745, de 9 de dezembro de 1993, que dispõe sobre a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, nos termos do inciso IX do art. 37 da Constituição Federal, e dá outras providências;

III. Lei nº 9.962, de 22 de fevereiro de 2000, que disciplina o regime de emprego público do pessoal da Administração Federal Direta, Autárquica e Fundacional, e dá outras providências;

IV. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

V. Decreto nº. 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

VI. Decreto nº. 4.073, de 3 de janeiro de 2002, que regulamenta a Lei nº. 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

VII. Decreto nº. 7.724, de 16 de maio de 2012, que regulamenta a Lei 12.527, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;

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

IX. Resolução nº 20, de 16 de julho de 2004, do Conselho Nacional de Arquivos, que dispõe sobre a inserção dos documentos digitais em programas de gestão arquivística de documentos dos órgãos e entidades integrantes do Sistema Nacional de Arquivos;

X. Resolução nº 32, de 17 de maio de 2010, do Conselho Nacional de Arquivos, que dispõe sobre a inserção dos metadados na Parte II do modelo de requisitos para sistemas informatizados de gestão arquivística de documentos - e-ARQ Brasil;

XI. Câmara Técnica de Documentos Eletrônicos. Conselho Nacional de Arquivos. e-ARQ Brasil: modelo de requisito para sistemas informatizados de gestão arquivística de documentos. Rio de Janeiro: Arquivo Nacional, 2011. v. 1.1;

XII. Câmara Técnica de Documentos Eletrônicos. Conselho Nacional de Arquivos. Glossário de termos técnicos (v5). 2010b;

XIII. Instrução Normativa nº. 01, de 13 de junho de 2008, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a gestão de segurança da informação e comunicações na Administração Pública Federal, direta e indireta, e dá providencias;

XIV. Instrução Normativa nº. 02, de 5 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

XV. Instrução Normativa nº. 03, de 6 de março de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal;

XVI. Norma Complementar nº. 03 da IN 01, de 30 de junho de 2009, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para elaboração da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal;

XVII. Norma Complementar nº. 04 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta;

XVIII. Norma Complementar nº 05 da IN 01, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal;

XIX. Norma Complementar nº. 06 da IN 01, de 11 de novembro de 2009, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre a gestão de continuidade de negócios em segurança da informação e comunicações;

XX. Norma Complementar nº. 07 da IN 01, de 06 de maio de 2010, do Gabinete de Segurança Institucional da Presidência da República, que estabelece diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações;

XXI. Norma Complementar nº. 09 da IN 01, de 15 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que estabelece orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações;

XXII. Portaria nº 14, de 21 de outubro de 2011, da Secretaria Executiva do Ministério da Ciência, Tecnologia e Inovação, que designa o Gestor de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação;

XXIII. Portaria nº 27, de 3 de fevereiro de 2012, do Ministério do Planejamento, Orçamento e Gestão, que aprova a atualização da Política de Segurança da Informação e Comunicações do Ministério do Planejamento Orçamento e Gestão;

XXIV. Portaria nº 383, de 30 de maio de 2012, do Gabinete do Ministro do Ministério da Ciência, Tecnologia e Inovação, que institui o Comitê Executivo de Tecnologia da Informação (CETI);

XXV. Portaria nº 384, de 30 de maio de 2012, do Gabinete do Ministro do Ministério da Ciência, Tecnologia e Inovação, que institui o Comitê de Segurança da Informação e Comunicações (CSIC);

XXVI. Portaria nº 165, de 30 de novembro de 2012, da Subsecretaria de Planejamento, Orçamento e Administração do Ministério da Ciência, Tecnologia e Inovação, que institui a Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS);

XXVII. Portaria nº 293, de 1º de abril de 2013, do Gabinete do Ministro do Ministério da Ciência, Tecnologia e Inovação, que institui a Política de Gestão Documental no âmbito do MCTI;

XXVIII. NBR ISO/IEC 27001:2006: Sistemas de Gestão de Segurança da Informação;

XXIX. NBR ISO/IEC 27002:2007: Código de Prática para a Gestão da Segurança da Informação.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 10 A segurança da informação e comunicações do Ministério da Ciência, Tecnologia e Inovação deve obedecer aos princípios do acesso, da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, da privacidade, da auditabilidade, e do não repúdio.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 11 A segurança da informação e comunicações tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes. (Ref. ISO/IEC 27002:2006).

Art. 12 As diretrizes de segurança da informação e comunicações devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e a estrutura do Ministério.

Art. 13 As diretrizes de segurança da informação e comunicações descritas nesta Política devem ser observadas por todos os usuários que executem atividades vinculadas a este Ministério durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 14 O cumprimento desta Política, bem como dos normativos que a complementam deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação e Comunicações (CSIC), buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 15 O Ministério deve observar as diretrizes estabelecidas nesta Política e deve se orientar pelas melhores práticas e procedimentos de segurança da informação e comunicações recomendados por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 16 O Ministério deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 17 É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo Ministério.

Parágrafo único. Cópias de documentos classificados deverão sofrer o mesmo processo de classificação de seu original.

Art. 18 O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor do ativo de informação é o próprio custodiante.

Art. 19 Os contratos, convênios, acordos e instrumentos congêneres firmados pelo Ministério devem conter cláusulas que determinem a observância desta Política e seus documentos complementares.

CAPÍTULO VI

DAS DIRETRIZES ESPECÍFICAS

Art. 20 Para cada uma das diretrizes constantes das seções deste capítulo deve ser observada a pertinência de elaboração de políticas, procedimentos, normas, orientações e/ou manuais

que disciplinem ou facilitem o seu entendimento.

Seção I

DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 21 A Gestão de Segurança da Informação e Comunicações (GSIC) deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação e comunicações.

Art. 22 A Gestão da Segurança da Informação e Comunicações (GSIC) deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à segurança da informação e comunicações, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos requisitos mínimos de qualidade e reflitam as necessidades operacionais do Ministério.

Parágrafo único. De forma a promover a gestão e fomentar os aspectos de segurança da informação, o Ministério deve:

I. definir uma Estrutura para a Gestão de Segurança da Informação e Comunicações (GSIC);

II. instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

III. instituir Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) em todos os seus órgãos e unidades;

IV. estabelecer a CPADS como órgão de assessoramento permanente do Comitê de Segurança da Informação (CSIC), sem prejuízo das atribuições propostas no artigo 34 do Decreto nº. 7.724, de 16 de maio de 2012.

Seção II

DA PROPRIEDADE DA INFORMAÇÃO

Art. 23 As informações geradas, adquiridas ou custodiadas sob a responsabilidade do Ministério são consideradas parte do seu patrimônio intelectual não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei de Inovação e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta Política, em seus documentos complementares e demais regulamentações em vigor.

Art. 24 É vedada a utilização de informações produzidas por terceiros para uso exclusivo do Ministério em quaisquer outros projetos ou atividades de uso diverso ao originalmente estabelecido, salvo autorização específica emitida pelo gestor do ativo de informação, nos processos e documentos de sua competência, ou pelo Ministro, nos demais casos, observando a legislação em vigor.

Seção III

DOS CONTROLES DE ACESSO

Art. 25 Devem ser registrados eventos relevantes, previamente definidos, para a segurança e o rastreamento de acesso às informações.

Art. 26 Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 27 Todos os sistemas de informação do Ministério, automatizados ou não, devem ter um custodiante do ativo da informação, formalmente designado pelo gestor do ativo de informação, que deve definir os privilégios de acesso às informações, observando a legislação em vigor.

Art. 28 O usuário é responsável por todos os atos praticados com suas identificações, entre as quais se destacam: nome do usuário na rede, carimbo, crachá, endereço de correio eletrônico e assinatura digital. O usuário responderá pela segurança dos ativos; dos processos que estejam sob sua responsabilidade e por todos os atos executados com suas identificações, salvo se comprovado que o fato ocorreu sem o conhecimento ou consentimento do usuário.

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

Art. 29 A autorização, o acesso e o uso da informação e dos recursos de tecnologia da informação e comunicações devem ser controlados e limitados ao necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de autorização, acesso ou uso necessitará de prévia autorização do gestor do ativo de informação, observando-se a legislação em vigor.

Parágrafo único. A autorização de que trata o *caput* poderá ser delegada ao custodiante do ativo de informação.

Art. 30 Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser adequados imediatamente, devendo ser cancelados em caso de desligamento do Ministério.

Seção IV

DA GESTÃO DE ATIVOS DA INFORMAÇÃO

Art. 31 Os ativos de informação devem:

I. ser inventariados e protegidos;

II. ter identificados, formalmente, o gestor do ativo de informação e o custodiante do ativo de informação;

III. ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV. ter a sua entrada e saída nas dependências dos órgãos e unidades citados no art. 5º autorizadas e registradas pelo gestor do ativo de informação:

a. ativos em suporte físico, ostensivos ou com restrição de acesso, deverão ter sua tramitação registrada em sistema de protocolo corporativo;

b. ativos em suporte físico sob restrição de acesso somente poderão ser apensados ao sistema de protocolo corporativo caso estejam criptografados;

c. ativos em suporte digital poderão ser tramitados por meio de sistema de protocolo corporativo ou por correio eletrônico;

d. ativos em suporte digital sob restrição de acesso somente poderão ser tramitados por sistema de protocolo ou por correio eletrônico quando criptografados e com autorização de seu gestor:

i. cópias digitais de ativos sob restrição de acesso para mecanismos de armazenamento de qualquer tipo estarão sujeitos às mesmas regras e restrições de seus originais;

ii. ativos classificados, para tramitar eletronicamente, deverão ter autorização expressa da autoridade classificadora, posto que sua tramitação pode gerar cópia eletrônica do ativo;

iii. ativos de informação sob restrição de acesso devem ser tramitados de forma segura, de maneira a garantir que seu conteúdo somente possa ser visto pelo destinatário autorizado, conforme especificado na Seção IV do Capítulo III do Decreto nº. 7.845, de 14 de novembro de 2012.

V. ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI. ser regulamentados por norma específica quanto a sua utilização e movimentação;

VII. ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 32 Os gestores do ativo de informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a realização de atividades no Ministério, observadas as normas de segurança da informação e comunicações.

Art. 33 Os recursos tecnológicos e as instalações de infraestrutura devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 34 Os sistemas de informação e as aplicações do Ministério devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Art. 35 O acesso dos usuários aos ativos de informação e sua utilização, quando autorizados, deve ser condicionado ao aceite a Termo de Responsabilidade, observando a legislação em vigor.

Seção V

DA GESTÃO ARQUIVÍSTICA DE DOCUMENTOS ELETRÔNICOS

Art. 36 A Gestão Arquivística de Documentos Eletrônicos tem por objetivo a produção/criação, uso/acesso, avaliação e destinação (arquivamento ou descarte) dos documentos eletrônicos autênticos e fidedignos.

Art. 37 Os documentos eletrônicos produzidos no âmbito do Ministério terão garantia de autoria, autenticidade e integridade asseguradas, nos termos da lei, mediante utilização de assinatura eletrônica.

Seção VI

DA GESTÃO ARQUIVÍSTICA DE CORREIO ELETRÔNICO

Art. 38. As mensagens de correio eletrônico de caráter institucional deverão ser reconhecidas como documento de arquivo, dotadas das qualidades inerentes a este, quais sejam: organicidade, unicidade, confiabilidade, autenticidade e acessibilidade, pois aquelas, também,

refletem as ações e as competências e servem de apoio às funções e às atividades do Ministério, logo deverão estar sob o alcance desta Política.

Seção VII

DA PRESERVAÇÃO DOS DOCUMENTOS EM MEIO ELETRÔNICO

Art. 39 O tratamento arquivístico – inclusive descarte – de documentos eletrônicos deve observar procedimentos definidos na legislação.

Parágrafo único. A gestão de documentos eletrônicos orienta-se pelos critérios da integridade e da disponibilidade das informações produzidas e custodiadas no âmbito do Ministério, respeitados os requisitos legais e os princípios de segurança da informação.

Art. 40. Os documentos constantes da base de dados corporativa devem ser armazenados em equipamentos e mídias que permitam acesso com celeridade compatível com as necessidades do negócio no âmbito do Ministério.

Art. 41. Ato do Ministro definirá Plano de Preservação de Documentos Eletrônicos, a partir de proposta formulada pelo Comitê de Segurança da Informação e Comunicações (CSIC), ouvida a Comissão Permanente de Avaliação de Documentos (CPAD).

Parágrafo único. O Plano de Preservação de Documentos Eletrônicos deve conter, entre outros elementos, a política de cópias de segurança (backup) e de recuperação em casos de perda de informação, bem como de retenção de versões de documentos eletrônicos.

Seção VIII

DA CLASSIFICAÇÃO DA INFORMAÇÃO

Art. 42 Informações geradas, adquiridas ou custodiadas pelo Ministério podem possuir classificação para indicar a necessidade, a prioridade e o nível esperado de proteção quanto ao seu tratamento. Quando classificadas serão observadas as exigências das atividades da instituição, considerando as implicações que um determinado grau de classificação trará para os seus objetivos institucionais e observando a legislação em vigor.

§ 1º Todo usuário deve ser capaz de identificar a classificação atribuída a uma informação tratada pelo Ministério e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

§ 2º A classificação deve auxiliar os gestores na priorização de ações e investimentos para a correta aplicação de mecanismos de tratamento.

Seção IX

DA GUARDA E TRAMITAÇÃO DE ATIVO DE INFORMAÇÃO SOB RESTRIÇÃO DE ACESSO

Art. 43 Ativos de informação sob restrição de acesso devem ser armazenados em local que garanta sua acessibilidade apenas a usuário autorizado.

§ 1º Se o ativo estiver em suporte impresso, deverá ser armazenado em arquivo com proteção de acesso.

§ 2º Se o ativo estiver em meio eletrônico, deve ser armazenado criptografado, utilizando-se o algoritmo de Estado.

Seção X

DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 44 O Comitê de Segurança da Informação e Comunicações (CSIC) deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

Parágrafo único. Os mecanismos de proteção estabelecidos devem estar alinhados aos riscos identificados.

Seção XI

DA SEGURANÇA EM RECURSOS HUMANOS

Art. 45 Os usuários devem ter ciência:

I - das ameaças e preocupações relativas à segurança da informação e comunicações;

II - de suas responsabilidades e obrigações no âmbito desta Política.

Art. 46 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. 47 Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários do Ministério, de acordo com suas competências funcionais.

Seção XII

DA GESTÃO DE RISCOS

Art. 48 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 comunicações.

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

Seção XIII

DA CONTINUIDADE DE NEGÓCIO

Art. 49 O Comitê de Segurança da Informação e Comunicações (CSIC) deverá instituir, formalmente, grupo de trabalho com objetivo de propor, manter e periodicamente testar medidas de gestão da continuidade e recuperação da informação, visando reduzir para um nível aceitável ou previamente definido a possibilidade de interrupção ou o impacto causado por

desastres nos recursos de tecnologia da informação e comunicações que suportam os processos vitais do Ministério, até que se retorne à normalidade.

Seção XIV

DO TRATAMENTO DE INCIDENTES DE REDE

Art. 50 O Comitê de Segurança da Informação e Comunicações (CSIC) deverá instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), em conformidade com a Norma Complementar nº NC05/IN01/DSIC/GSIPR.

Seção XV

DA CRIPTOGRAFIA

Art. 51 O uso de recursos criptográficos interfere na disponibilidade, integridade, confidencialidade e autenticidade das informações, sendo, portanto, responsabilidade do Comitê de Segurança da Informação e Comunicações (CSIC) a implementação dos procedimentos relativos ao seu uso, no âmbito das informações geradas, adquiridas ou custodiadas sob a responsabilidade do Ministério, em conformidade com as orientações contidas em norma específica.

Art. 52 O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Sigilo e de Responsabilidade por seu uso.

Seção XVI

DA AUDITORIA E CONFORMIDADE

Art. 53 A autorização, o acesso e o uso da informação e dos procedimentos de auditoria devem ser executados nos recursos de tecnologia da informação e comunicações.

Art. 54 Deve ser realizada, com periodicidade mínima de três anos, verificação de conformidade das práticas de segurança da informação e comunicações do Ministério com esta Política, com suas normas e com seus procedimentos complementares, bem como com a legislação específica de segurança da informação e comunicações.

Art. 55 A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o Ministério.

Art. 56 A verificação da conformidade será realizada de forma planejada, mediante calendário de ações aprovado pelo CSIC.

Art. 57 O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 58 Nenhum órgão ou unidade, abrangidos por esta Política, poderá permanecer sem verificação de conformidade de suas práticas de segurança da informação e comunicações por período superior a 3 (três) anos.

Art. 59 A execução da verificação de conformidade será realizada por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação e Comunicações (CSIC), podendo, com a prévia aprovação deste, ser subcontratada no todo ou em parte.

Art. 60 É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 61 A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 62 Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de Segurança da Informação e Comunicações ao gestor do ativo de informação do órgão ou unidade verificada, para ciência e tomada das ações cabíveis.

Seção XVII

DO PLANO DE INVESTIMENTOS EM SIC DO MCTI

Art. 63 Os investimentos em SIC serão realizados de forma planejada e consolidados em um plano de investimentos.

Art. 64 O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 65 Os investimentos em segurança da informação e comunicações deverão estar prevista na Lei Orçamentária Anual (LOA).

Art. 66 O plano de investimentos, assim como a correspondente proposta orçamentária, serão aprovados no âmbito do Comitê de Segurança da Informação e Comunicações (CSIC) e submetidos à aprovação do Secretário-Executivo do Ministério.

Art. 67 Caso a dotação concedida na Lei Orçamentária Anual (LOA) seja inferior à solicitada na proposta orçamentária, ou haja limitação na execução orçamentária, caberá ao Comitê de Segurança da Informação e Comunicações (CSIC) realizar a correspondente revisão do plano de investimentos.

Seção XVIII

DA RELAÇÃO COM TERCEIROS

Art. 68 Nos editais de licitação, nos contratos, contratos de gestão, convênios, acordos e instrumentos congêneres de cooperação técnica com entidades prestadoras de serviços para o Ministério deverá constar cláusula específica sobre a obrigatoriedade de observância a esta Política, bem como deverá ser exigida, da entidade contratada, a assinatura do Termo de Responsabilidade.

Art. 69 O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas e procedimentos complementares aos seus empregados e prepostos envolvidos em atividades no Ministério.

CAPÍTULO VII

DAS SANÇÕES

Art. 70 A não observância desta Política e/ou de seus documentos complementares, bem como a quebra de controles de segurança da informação e comunicações, poderá acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VIII

DAS COMPETÊNCIAS E RESPONSABILIDADE

Seção I

DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 71 As competências do Comitê de Segurança da Informação e Comunicações (CSIC) do Ministério da Ciência, Tecnologia e Inovação estão descritas na Portaria MCTI nº 384, de 30 de maio de 2012, a saber**:**

I. assessorar na implementação das ações de segurança da informação e comunicações do Ministério;

II. minutar Política de Segurança da Informação composta por políticas, diretrizes, normas e procedimentos relativos à segurança da informação e comunicações para o Ministério, em conformidade com as legislações existentes sobre o tema, submetendo-a a Presidência do Comitê Executivo de Tecnologia da Informação, que a integrará à Política de Informação vigente, submetendo-as à apreciação da autoridade competente;

III. propor alterações na Política de Segurança da Informação e Comunicações;

IV. instituir Grupos de Trabalho, em caráter permanente ou temporário, para tratar de temas específicos relacionados à segurança da informação e comunicações;

V. receber e analisar as comunicações referentes à quebra de segurança, apresentando parecer à autoridade/órgão competente para análise e providências;

VI. apoiar a implementação de programas destinados a conscientização e à capacitação de recursos humanos em segurança da informação e comunicações;

VII. apresentar soluções técnicas de arquitetura e infraestrutura vinculadas à segurança da informação e comunicações;

VIII. elaborar seu regimento interno no prazo de 180 (cento e oitenta) dias, contados da sua instalação e submetê-lo à aprovação do Secretário-Executivo do Ministério;

IX. exercer outras responsabilidades que lhe forem atribuídas em regimento interno.

Seção II

DO GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 72 As competências do Gestor da Segurança da Informação e Comunicações do Ministério estão descritas na Portaria SEXEC/MCTI nº 14, de 21 de outubro de 2011, a saber:

I. promover cultura de segurança da informação e comunicações;

II. acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III. propor recursos necessários às ações de segurança da informação e comunicações;

IV. coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

V. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI. manter contato direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR) para o trato de assuntos relativos à segurança da informação e comunicações;

VII. propor normas e procedimentos relativos à segurança da informação e comunicações.

Seção III

DOS USUÁRIOS

Art. 73 Compete aos usuários do Ministério da Ciência, Tecnologia e Inovação:

I. cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações do Ministério da Ciência, Tecnologia e Inovação;

II. buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III. assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia e Inovação (Posic/MCTI), bem como assumindo responsabilidade por seu cumprimento;

IV. proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pelo Ministério;

V. assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Ministério;

VI. comunicar imediatamente ao Comitê de Segurança da Informação e Comunicações (CSIC) qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

CAPÍTULO IX

DA VIGÊNCIA E ATUALIZAÇÃO

Art. 74 Esta Política bem como o conjunto de instrumentos normativos gerados a partir dela, será revisada de forma periódica ou sempre que se fizer necessário, não excedendo o período máximo de dois anos.

Art. 75 Esta Portaria entra em vigor na data de sua publicação.

MARCO ANTONIO RAUPP

Publicada no D.O.U. de 06.09.2013,Seção I, Pág. 7.