MINISTÉRIO DA INTEGRAÇÃO NACIONAL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES

PRINCÍPIOS E DIRETRIZES

SETEMBRO 2013

Sumário

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DAS COMUNICAÇÕES DO MINISTÉRIO DA INTEGRAÇÃO NACIONAL

1.1. ESCOPO

A Política de Segurança da Informação e das Comunicações (POSIC) tem por finalidade estabelecer as diretrizes para a segurança do manuseio, tratamento e controle e para a proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio, devendo estas diretrizes serem observadas na definição de regras operacionais e procedimentos no âmbito do Ministério da Integração Nacional (MI).

A Política de Segurança da Informação e das Comunicações obedecerá aos princípios constitucionais, administrativos e ao arcabouço legislativo vigente que rege a Administração Pública Federal.

1.2. ABRANGÊNCIA

Essa Política aplica-se a todos as unidades administrativas do MI, servidores, funcionários e colaboradores externos que prestam serviço em razão de contratos administrativos firmados na forma da Lei e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas na celebração de parcerias, acordos de cooperação de qualquer tipo, convênios e termos congêneres.

1.3. CONCEITOS E DEFINIÇÕES

Para os fins dessa Política, consideram-se os conceitos dos termos e expressões que constam do glossário de Segurança da Informação e das Comunicações:

Agente Público – aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao MI;

Ameaça – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;

Ativo – qualquer bem, tangível ou intangível, que tenha valor para a organização;

Ativo da Informação – os 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;

Ativo Sigiloso – qualquer bem tangível ou intangível que possa conter informações sigilosas que, se acessadas por pessoas não autorizadas, podem causar danos significativos à organização;

Autenticação – é o ato de confirmar que algo ou alguém é autêntico, ou seja, uma garantia de que qualquer alegação de ou sobre um objeto é verdadeira;

Autenticidade – propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

Classificação da informação – atribuição, pela autoridade competente, de grau de sigilo dado à informação, documento, material, área ou instalação;

Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

Contingência – descrição de medidas a serem tomadas por uma organização, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos;

Controle de Acesso – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

Cópia de Segurança – copiar dados em um meio separado do original, de forma a protegê-los de qualquer eventualidade;

Credenciais ou contas de acesso – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha;

Criptografia – é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da chave criptográfica);

CETI – Comitê Estratégico de Tecnologia da Informação do MI;

Disponibilidade – propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

DGE – Departamento de Gestão Estratégica;

DSIC – Departamento de Segurança da Informação e das Comunicações do Gabinete de Segurança Institucional – GSI;

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

Gestão de Continuidade de Negócios – Processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, se concretizando, poderiam causar, e fornecendo e mantendo um nível aceitável de serviço em face de rupturas e desafios à operação normal do dia-a-dia;

Gestão de Risco – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Gestão de Segurança da Informação e das Comunicações – conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

Gestor da Informação – pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;

Gestor de Segurança da Informação e das Comunicações – é responsável pelas ações de segurança da informação e das comunicações no âmbito do órgão ou entidade da APF;

Informação – dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Informações Críticas – são as informações de extrema importância para a sobrevivência da instituição;

Informação sigilosa – informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

Perfil de acesso – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;

Plano de Continuidade de Negócios – documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, num nível previamente definido, em casos de incidentes;

Quebra de segurança – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

Segurança da Informação e das Comunicações – ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

Sistema de Segurança da Informação – proteção de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento;

Termo de Responsabilidade – 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;

Tratamento da informação – recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

Tratamento de Incidentes de Segurança em Redes Computacionais – serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as

análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

Usuários – servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso os Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade;

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.

1.4. REFERÊNCIAS LEGAIS E NORMATIVAS

Lei nº 9.983, de 14 de julho de 2000: Altera o Decreto Lei nº 2848/40 – Código Penal, sobre tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

Lei n° 9.610, de 19 de fevereiro de 1998, que altera, atualiza e consolida a legislação sobre direitos autorais;

Lei 10.683 de 28 de maio de 2003 – Art. 6º, competência do Gabinete de Segurança Institucional da Presidência da República;

Decreto nº 7.724 de 16/05/2012, que regulamenta a Lei 12.527, de 18/11/2011 – Dispõe sobre o acesso a informações;

Decreto nº 6.931, de 11 de agosto de 2009 - art. 8º do Anexo I – competência do Departamento de Segurança da Informação e Comunicações;

Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse de segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

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;

Decreto 1.171, de 24 de junho de 1994 que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, e outras providências;

Instrução Normativa GSI Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal;

Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização;

Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações;

Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal;

Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC nos órgãos e entidades da Administração Pública Federal;

Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal;

Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

Norma Complementar nº 07/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

Norma Complementar nº 09/IN01/DSIC/GSIPR, Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta;

NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão da Segurança da Informação;

NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação;

NBR/ISO/IEC 27001/2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação;

ISO/IEC Guide 73:2002 - Gestão de Riscos / Vocabulário – Recomendações para uso em normas;

Norma NBR/ISO/IEC 27005:2011 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação (SI);

Código Civil, Art. 1.016, que institui que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções.

1.5. PRINCÍPIOS

São princípios da POSIC:

1.5.1. Responsabilidade: os agentes públicos devem conhecer e respeitar a POSIC do MI e devem ser responsabilizados pelos atos que comprometem a segurança da informação;

1.5.2. Ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da segurança da informação e das comunicações;

1.5.3. Celeridade: as ações de segurança da informação e das comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;

1.5.4. Economicidade da proteção dos ativos de informação;

1.5.5. Clareza: as regras de segurança da informação e das comunicações devem ser precisas, concisas e de fácil entendimento;

1.5.6. Privacidade: informação que fira o respeito à intimidade e à honra dos cidadãos não pode ser divulgada;

1.5.7. Pessoalidade e utilidade do acesso aos ativos de informação; e

1.5.8. Publicidade: dar transparência no trato da informação, observados os critérios legais;

1.5.9. Serão observados ainda, sem prejuízo das demais, outros princípios constitucionais que regem a Administração Pública Federal – APF.

1.6. PRECEITOS

São preceitos da POSIC:

1.6.1. Menor privilégio: Usuários e sistemas devem ter a menor autoridade e o mínimo acesso aos recursos necessários para realizar uma dada tarefa;

1.6.2. Segregação de função: Funções de planejamento, execução e controle devem ser segregadas de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos;

1.6.3. Auditabilidade: Todos os eventos significantes de sistemas e processos devem ser rastreáveis até o evento inicial;

1.6.4. Mínima dependência de segredos: Os controles deverão ser efetivos ainda que a ameaça saiba de suas existências e como eles funcionam;

1.6.5. Controles automáticos: Sempre que possível, controles de segurança automáticos deverão ser utilizados;

1.6.6. Resiliência: Os sistemas e processos devem ser projetados para que possam resistir ou se recuperarem dos efeitos de um desastre;

1.6.7. Defesa em profundidade: Controles devem ser desenhados em camadas de tal forma que quando uma camada de controle falhar, haja um tipo diferente de controle em outra camada para prevenir a brecha de segurança;

1.6.8. Exceção aprovada: Exceções à POSIC deverão sempre ter aprovação superior;

1.6.9. Substituição da segurança em situações de emergência: Controles somente devem ser desconsiderados de formas predeterminadas e seguras. Devem sempre existir procedimentos e controles alternativos para minimizar o nível de risco em situações de emergência.

1.7. DIRETRIZES GERAIS

São diretrizes gerais da POSIC:

1.7.1. A Política de Segurança da Informação é o instrumento que regula a proteção dos dados, informações e conhecimentos da Instituição, com vistas à garantia de integridade, disponibilidade, conformidade e confidencialidade;

1.7.2. Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio (regular exercício das funções institucionais);

1.7.3. O gerenciamento dos ativos de informação deverá observar normas operacionais e procedimentos específicos, a fim de garantir sua operação segura e contínua;

1.7.4. O cumprimento dessa Política, bem como das normas complementares e procedimentos de Segurança da Informação no MI será auditado periodicamente, de acordo com os critérios definidos pelo CETI;

1.7.5.O MI deve criar e manter registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna do MI;

1.7.6. As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com valor do ativo protegido;

1.7.7. O acesso às informações sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento;

1.7.8. Todos os membros, servidores e estagiários do MI e demais agentes públicos ou particulares que, oficialmente, executem atividade vinculada à atuação institucional do MI e sejam usuários dos ativos sigilosos, devem assinar Termo de Compromisso quanto ao sigilo dos dados, informações e conhecimentos do MI.

1.7.9. As responsabilidades pela segurança da informação devem ser definidas nas descrições de cargos e funções, bem como nos termos e condições das contratações que envolvam o manuseio de dados, informações ou conhecimentos do MI;

1.7.10. Todos os usuários devem ser conscientizados e treinados nos procedimentos de segurança da informação;

1.7.11. O controle operacional de uma atividade crítica não pode ser atribuição exclusiva de uma única pessoa;

1.7.12. Quando do afastamento, mudança de responsabilidades e de lotação ou atribuições dentro da organização faz se necessária a revisão imediata dos direitos de acesso e uso dos ativos;

1.7.13. Quando da efetivação do desligamento de usuário, deverão ser extintos todos os direitos de acesso e uso dos ativos a ele atribuído;

1.7.14. Todo ativo produzido pelo usuário desligado deverá ser mantido pela MI garantindo o reconhecimento e o esclarecimento da propriedade do acervo para Instituição;

1.7.15. As informações custodiadas ou de propriedade do MI devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor;

1.7.16. O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade;

1.7.17. A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte;

1.7.18. Todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade do MI e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

1.7.19. De forma a promover a gestão e fomentar os aspectos de segurança da informação, o MI deve instituir normas operacionais que estabeleçam procedimentos, processos e mecanismos que garantam o controle de acesso às informações, instalações e sistemas de informação.

1.8. COMPETÊNCIAS E RESPONSABILIDADES

1.8.1. Compete ao DGE

1.8.1.1. Assegurar que a implementação dos controles de segurança da informação tenha uma coordenação e permeie toda a organização;

1.8.1.2. Assegurar os recursos necessários para a implementação e gestão da POSIC do MI.

1.8.2. Compete ao CETI

1.8.2.1. Definir critérios para auditoria periódica destinada a aferir o cumprimento da POSIC do MI e suas Normas Operacionais;

1.8.2.2. Manifestar-se sobre a POSIC, com posterior encaminhamento ao DGE, para aprovação;

1.8.2.3. Designar o Gestor de Segurança da Informação e das Comunicações, o Comitê de SIC e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

1.8.3. Compete ao Comitê de SIC do MI

1.8.3.1 Assessorar na implementação das ações de segurança da informação e das comunicações;

1.8.3.2. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e das comunicações;

1.8.3.3. Propor alterações na POSIC;

1.8.3.4 Propor normas relativas à segurança da informação e das comunicações.

1.8.4. Compete ao Gestor de Segurança da Informação e das Comunicações do MI

1.8.4.1. Promover a cultura de segurança da informação e das comunicações;

1.8.4.2. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

1.8.4.3. Propor recursos necessários às ações de segurança da informação e das comunicações;

1.8.4.4. Coordenar o Comitê de SIC e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

1.8.4.5. Manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e das comunicações;

1.8.4.6. Propor normas relativas à segurança da informação e das comunicações;

1.8.4.7. Propor modificações à POSIC;

1.8.4.8. Definir estratégias para a implantação da POSIC;

1.8.4.9. Editar Normas Operacionais de Segurança da Informação e das Comunicações, cabendo ao CETI a recomendação de alteração normativa;

1.8.4.10. Planejar e coordenar a execução dos programas, planos, projetos e ações de segurança;

1.8.4.11. Apurar os incidentes de segurança críticos e encaminhar os fatos apurados para aplicação das penalidades previstas;

1.8.4.12. Supervisionar, analisar e avaliar a efetividade dos processos, procedimentos, sistemas e dispositivos de segurança da informação;

1.8.4.13. Manter a análise de risco atualizada, refletindo o estado corrente da organização;

1.8.4.14. Identificar controles físicos, administrativos e tecnológicos para mitigação do risco;

1.8.4.15. Recepcionar, organizar, armazenar e tratar adequadamente as informações de eventos e incidentes de segurança, determinando aos respectivos gestores as ações corretivas ou de contingência em cada caso;

1.8.4.16. Produzir relatórios síntese de incidentes de segurança da informação para o CETI.

1.8.5. Compete ao Gestor da Informação

1.8.5.1. Tratar e classificar a informação;

1.8.5.2. Definir os requisitos de segurança para os ativos sob sua responsabilidade;

1.8.5.3. Conceder e revogar acessos;

1.8.5.4. Autorizar a divulgação de informações.

1.9. SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO

1.9.1. Todas as unidades do MI deverão manter um processo permanente de divulgação de suas normas e procedimentos para capacitar, conscientizar e sensibilizar seus usuários à correta conduta na utilização das informações do MI.

1.10. PENALIDADES

1.10.1 O não cumprimento das determinações da POSIC sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do MI;

1.10.2 O descumprimento das disposições constantes nessa Política e nas Normas Operacionais sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil;

1.10.3 O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política,

fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente;

1.10.4 Os casos omissos e as dúvidas surgidas na aplicação dessa política serão submetidos ao CETI.

1.11. ATUALIZAÇÃO

1.11.1 Essa POSIC deve ser revisada e atualizada periodicamente no máximo a cada 3 (três) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

1.12. VIGÊNCIA

1.12.1 Esse documento entra em vigor na data de sua publicação.

1.13. DIVULGAÇÃO

1.13.1 Após a publicação desta Política de Segurança da Informação e das Comunicações, ela estará disponível permanentemente nos canais de comunicação interno e externo do MI e no D.O.U. a todos os usuários.

1.14. DISPOSIÇÕES FINAIS

1.14.1 Os casos omissos e as dúvidas com relação a essa POSIC serão submetidos ao Comitê de SIC ou Comitê Diretivo de TI do MI.