CAPÍTULO II
DO ESCOPO
Seção I
Dos Princípios

Art. 5º A POSIC/MJ é guiada pelos princípios da legalidade, segurança, publicidade, privacidade e ética.

Parágrafo único. Para efeitos da POSIC/MJ, entende-se por:

I - legalidade: observância dos parâmetros legais e regulamentares na implementação das ações de SIC;

II - segurança: proteção dos ativos de informação contra perda, corrupção, destruição, acesso, uso e alteração indevidos ou não autorizados;

III - publicidade: divulgação da POSIC/MJ e de todas as normas complementares aos agentes públicos em exercício no Ministério;

IV - privacidade: proteção do direito individual da pessoa à inviolabilidade de sua intimidade e vida privada e do sigilo de suas comunicações, observado o disposto no art. 31 da Lei nº 12.527, de 18 de novembro de 2011, e nos arts. 55 a 62 do Decreto nº 7.724, de 16 de maio de 2012; e

V - ética: observância do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171, de 22 de junho de 1994, e demais regras de conduta normativamente delimitadas para os agentes públicos.

Seção II
Das Diretrizes

Art. 6º São diretrizes gerais da POSIC/MJ:

I - estabelecer medidas e procedimentos de tratamento da informação, com o objetivo de viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

II - manter equipe de tratamento e resposta a incidentes em redes computacionais, com objetivo de registrar, analisar e tratar incidentes de SIC por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas;

III - elaborar e implementar plano de gestão de riscos, com o objetivo de reduzir as vulnerabilidades, evitar ameaças, minimizar a exposição aos riscos e atenuar os impactos associados aos ativos de informação do Ministério;

IV - elaborar e implementar plano de gestão de continuidade, com o objetivo de identificar ameaças e possíveis impactos na continuidade dos processos e serviços essenciais para o funcionamento do Ministério;

V - elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso aos ativos de informação e avaliar sua conformidade com as normas de SIC em vigor;

VI - implementar controle de acesso lógico aos sistemas de computação e redes de computadores e controle de acesso físico às instalações, com o objetivo de preservar os ativos de informação do Ministério;

VII - definir regras claras e precisas de uso do e-mail institucional, com o objetivo de evitar o uso para fins particulares, com abuso de direito ou violação à imagem do Ministério; e

VIII - controlar o acesso à Internet, com o objetivo de evitar que os recursos computacionais do Ministério sejam utilizados em desrespeito às leis, aos costumes e à dignidade da pessoa humana.

CAPÍTULO III
DAS PENALIDADES

Art. 7º A desobediência às regras da POSIC/MJ e demais normas complementares implicará em sanções administrativas, sem prejuízo da apuração nas esferas cível e penal.

CAPÍTULO IV
DA GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
Seção I
Do Gestor de Segurança da Informação e Comunicações

Art 8º A implementação da POSIC/MJ ficará a cargo do Gestor de Segurança da Informação e Comunicações, servidor público efetivo designado pelo Secretário-Executivo, cabendo-lhe especialmente:

I - examinar, formular, promover e coordenar as ações de SIC no Ministério, em articulação com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República;

II - acompanhar investigações e avaliações de danos decorrentes de quebras de segurança;

III - propor às autoridades competentes os recursos necessários às ações de SIC no Ministério;

IV - coordenar o Comitê Gestor de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Ministério da Justiça;

V - divulgar e supervisionar o cumprimento da POSIC/MJ e suas normas complementares;

VI - propor normas e procedimentos relativos à SIC no âmbito do Ministério; e

VII - resolver os casos omissos e as dúvidas surgidas na aplicação da POSIC/MJ e suas normas complementares.

Seção II
Do Comitê Gestor de Segurança da Informação e Comunicações

Art 9º Fica criado o Comitê Gestor de Segurança da Informação e Comunicações com a competência de:

I - assessorar na implementação das ações de SIC no Ministério;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

III - propor normas e procedimentos internos relativos à SIC, em conformidade com as legislações existentes sobre o tema;

IV - auxiliar na elaboração dos planos de gestão de riscos e de continuidade e na definição das diretrizes de auditoria e conformidade no âmbito do Ministério;

V - revisar a POSIC/MJ sempre que se fizer necessário;

VI - elaborar relatórios periódicos de suas atividades, encaminhando-os ao Secretário-Executivo; e

VII - indicar os integrantes da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

Art 10º O Comitê será composto por um representante de cada órgão e entidade a seguir indicados:

I - Gabinete do Ministro;
II - Secretaria-Executiva;
III - Secretaria Nacional de Justiça;
IV - Secretaria Nacional de Segurança Pública;
V - Secretaria de Reforma do Judiciário;
VI - Secretaria Nacional do Consumidor;
VII - Secretaria Nacional de Políticas sobre Drogas:
VIII - Secretaria Extraordinária de Segurança para Grandes Eventos;
IX - Departamento de Polícia Federal;
X - Departamento de Polícia Rodoviária Federal;
XI - Departamento Penitenciário Nacional;
XII - Defensoria Pública da União;
XIII - Arquivo Nacional;
XIV - Conselho Administrativo de Defesa Econômica; e
XV - Fundação Nacional do Índio.

§ 1º Os representantes do Comitê e seus suplentes serão designados mediante ato do Secretário-Executivo.

§ 2º A participação no Comitê será considerada serviço público relevante e não ensejará remuneração de qualquer espécie.

§ 3º O Comitê poderá convidar outros técnicos para colaborarem nos trabalhos a serem desenvolvidos, sem direito a voto.

§ 4º As deliberações do Comitê serão tomadas por maioria simples, presente a maioria absoluta de seus membros.

§ 5º O Comitê reunir-se-á a cada dois meses, podendo haver convocação extraordinária, a critério de seu coordenador.

Seção III
Da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

Art. 11º Fica criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, com competência de:

I - registrar, analisar e tratar eventos e incidentes de SIC, por meio da coleta de evidências, investigação de ataques, provimento de assistência local e remota e intermediação da comunicação entre as partes envolvidas;

II - coordenar, analisar e sugerir ações apropriadas para remoção de qualquer arquivo, objeto ou vulnerabilidade que possa causar prejuízos aos sistemas e redes de computadores ou quebra de segurança;

III - disseminar alertas de vulnerabilidades e outras notificações relacionadas à SIC no âmbito do Ministério;

IV - assessorar tecnicamente os órgãos e unidades do Ministério;

V - avaliar o emprego de ferramentas de SIC;

VI - avaliar e analisar riscos atuais e iminentes, bem como propor ações para sua mitigação;

VII - realizar testes para homologação dos sistemas de SIC do Ministério; e

VIII - realizar outras atribuições que lhe forem cometidas pelo Gestor de Segurança da Informação e Comunicações.

Parágrafo único. Os membros da ETIR deverão ter perfil técnico adequado às funções de tratamento de incidentes em redes computacionais.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 12º O acesso à Internet realizado por meio de ativos de tecnologia de informação e comunicações do Ministério deve ser autorizado, identificado e registrado.

Art. 13º Os registros de acessos aos ativos de informação do Ministério devem ser preservados em conformidade à legislação em vigor.

Art. 14º O conteúdo das comunicações, mensagens e arquivos, transitados ou produzidos por meio do correio eletrônico institucional é considerado propriedade do órgão, não sendo preservada a confidencialidade nos casos de violação da legislação em vigor.

Art. 15º As atribuições da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais serão exercidas pelo Grupo de Atendimento e Tratamento de Incidentes de Segurança da Informação - GATI do Ministério da Justiça.

Art. 16º A POSIC/MJ e suas normas complementares deverão ser revisadas sempre que se fizer necessário, não excedendo o período máximo de dois anos.

Art. 17º Ficam revogadas as Portarias nº 2.086, de 22 de novembro de 2005, e nº 279, de 10 de março de 2006, do Ministério da Justiça.

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

JOSÉ EDUARDO CARDOZO

ARQUIVO NACIONAL
CONSELHO NACIONAL DE ARQUIVOS

RESOLUÇÃO Nº 36, DE 19 DE DEZEMBRO DE 2012

Dispõe sobre a adoção das Diretrizes para a Gestão arquivística do Correio Eletrônico Corporativo pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR.

O PRESIDENTE DO CONSELHO NACIONAL DE ARQUIVOS - CONARQ, no uso de suas atribuições, previstas no item IX do art. 23 de seu Regimento Interno, aprovado pela Portaria nº 2.588, do Ministério da Justiça, de 24 de novembro de 2011, em conformidade com a deliberação do Plenário em sua 68ª reunião plenária do CONARQ, realizada no dia 5 de dezembro de 2012 e,

Considerando que o Conselho Nacional de Arquivos tem por finalidade definir a política nacional de arquivos públicos e privados e exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo, independente da forma ou do suporte em que a informação está registrada;

Considerando o estabelecido na Resolução nº 20, do CONARQ, de 16 de julho de 2004, 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;

Considerando que o correio eletrônico corporativo tem sido utilizado para a transmissão e recebimento de mensagens no curso das atividades desenvolvidas pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR, resolve:

Art. 1º Aprovar as Diretrizes para a Gestão Arquivística do Correio Eletrônico Corporativo, a ser adotado pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR, e disponibilizado no sitio do CONARQ, em: <http://www.conarq.arquivonacional.gov.br>.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

JAIME ANTUNES DA SILVA

RESOLUÇÃO Nº 37, DE 19 DE DEZEMBRO DE 2012

Aprova as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais.

O PRESIDENTE DO CONSELHO NACIONAL DE ARQUIVOS - CONARQ, no uso de suas atribuições, previstas no item IX do art. 23 de seu Regimento Interno, aprovado pela Portaria nº. 2.588, do Ministério da Justiça, de 24 de novembro de 2011, em conformidade com a deliberação do Plenário em sua 68ª reunião plenária do CONARQ, realizada no dia 5 de dezembro de 2012,

Considerando que é dever do Poder Público a gestão documental, a proteção especial aos documentos de arquivo e as providências para franquear aos cidadãos as informações contidas na documentação governamental;

Considerando que o Conselho Nacional de Arquivos tem por finalidade definir a política nacional de arquivos públicos e privados e exercer orientação normativa visando à gestão documental e à proteção especial aos documentos de arquivo, independentemente da forma ou do suporte em que a informação está registrada;

Considerando que a organização dos arquivos e o gerenciamento das informações neles contidas se constituem em instrumento de eficácia administrativa, contribuindo para a modernização da administração pública;

Considerando que as organizações públicas e privadas e os cidadãos vêm cada vez mais produzindo documentos arquivísticos digitais e que governos, organizações e cidadãos dependem do documento digital como fonte de prova e de informação, e para garantia de direitos;

Considerando que os documentos arquivísticos digitais podem se apresentar na forma de texto, imagem fixa ou em movimento, áudio, base de dados, planilha e outras num repertório crescente de possibilidades;

Considerando que os documentos digitais são suscetíveis à alteração, lícita ou ilícita, à degradação física e à obsolescência tecnológica de hardware, software e formatos, as quais podem colocar em risco sua autenticidade;

Considerando que a gestão arquivística de documentos, independentemente da forma ou do suporte adotados, tem por objetivo garantir a produção, a manutenção e a preservação de documentos arquivísticos confiáveis e autênticos;

Considerando o conceito de autenticidade dos documentos a partir da Arquivologia e da Diplomática;

Considerando a Resolução nº 24, de 3 de agosto de 2006, que estabelece diretrizes para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas públicas, resolve:

Art. 1º Aprovar as Diretrizes para a Presunção de Autenticidade de Documentos Arquivísticos Digitais, disponibilizadas no sitio do CONARQ, em: <http://www.conarq.arquivonacional.gov.br>.

§ 1º As Diretrizes de que trata essa resolução têm por finalidade instrumentalizar os produtores e custodiadores de documentos arquivísticos para essa presunção da autenticidade desses documentos.