UNIVERSIDADE FEDERAL DA PARAÍBA - UFPB
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE ARQUIVOLOGIA

François Braga de Azevedo Filho

O correio eletrônico corporativo na perspectiva da gestão documental e da segurança da informação: uma análise de práticas do poder executivo federal.

JOÃO PESSOA
2015

UNIVERSIDADE FEDERAL DA PARAÍBA - UFPB
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE ARQUIVOLOGIA

François Braga de Azevedo Filho

O correio eletrônico corporativo na perspectiva da gestão documental e da segurança da informação: uma análise de práticas do poder executivo federal

Monografia apresentada ao Curso de Graduação em Arquivologia da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de bacharel em Arquivologia.

Orientadora: Profa. Ms. Julianne Teixeira e Silva

JOÃO PESSOA
2015

Dados Internacionais de Catalogação na Publicação (CIP)

A994c Azevedo Filho, François Braga de.

O correio eletrônico corporativo na perspectiva da gestão documental e da segurança da informação: uma análise de práticas do poder executivo federal./ François Braga de Azevedo Filho. – João Pessoa: UFPB, 2015.

150f.: il.

Orientador: Profª. Ms. Julianne Teixeira e Silva.

Trabalho de conclusão de curso (Graduação em Arquivologia) – UFPB/CCSA.

1. Gestão de documentos. 2. Correio Eletrônico. 3. Segurança da informação. 4. Órgão público federal. I. Título.

UFPB/CCSA/BS CDU: 930.25:004773.3(043.2)

O correio eletrônico corporativo na perspectiva da gestão documental e da segurança da informação: uma análise de práticas do poder executivo federal

FRANÇOIS BRAGA DE AZEVEDO FILHO

Aprovado em 21 de Dezembro de 2015.

BANCA EXAMINADORA

Ms. Julianne Teixeira e Silva (Orientadora)

Dra. Rosilene Agapito da Silva Llarena

Dr. Wagner Junqueira de Araújo

À minha família, em especial aos meus pais, François Braga e Ana Maria Lucena, por todo sacrifício feito por mim.

AGRADECIMENTOS

Quero, antes de tudo, agradecer a Deus pela força e providência nestes últimos tempos e pela graça de superar desafios que a vida me reservou.

Agradeço à Universidade Federal da Paraíba, em especial ao seu corpo docente. Não pretendendo aqui citar nomes, pois tenho um grande sentimento de gratidão principalmente àqueles que se dedicaram de forma especial e particular a nos tornar profissionais capacitados e que oferecem o diferencial no mercado de trabalho. Para além disso, nos mostraram a importância da docência, despertando o desejo de um dia estar entre eles exercendo este papel tão importante na sociedade. Um agradecimento também especial à Coordenação de Arquivologia e seus técnico-administrativos, que tanto se esforçaram quando precisei, e à minha turma (as aulas não seriam tão divertidas sem vocês).

Quero agradecer à toda minha família pela presença e disposição em ajudar em todos os momentos de minha vida, principalmente nos mais complicados. E digo ainda que, se estou aqui hoje, é pelo incentivo e apoio que todos me deram, citando aqui a fundamental participação dos meus pais, François Braga e Ana Maria Lucena, e a compreensão e carinho da minha esposa Raissa e minha filha Marina, um dos meus maiores presentes até aqui.

Agradeço também a minha orientadora Profa. Julianne Teixeira por todo encorajamento, dedicação e força que depositou neste TCC e em mim. Agradeço a banca composta por Profa. Rosilene Agapito e Prof. Wagner Araújo, que prontamente atenderam ao meu convite e por suas considerações que tanto contribuíram para este trabalho.

E por último, a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

“Até aqui nos ajudou o Senhor.”
I Samuel 7:12b

RESUMO

Com o surgimento de noticias de espionagem norte americana sob as comunicações do governo federal brasileiro e de outros países, objetivou-se neste trabalho identificar quais medidas estão sendo tomadas pelo poder executivo federal apresentando a relação entre a segurança da informação e comunicação e a gestão documental. Utilizando-se das prerrogativas da Lei de Acesso, foram enviadas perguntas através do Serviço Eletrônico de Informação ao Cidadão a uma amostra de sete ministérios e a uma empresa pública, como forma de se obter informações sobre as medidas governamentais em respeito à segurança da informação nos correios eletrônicos corporativos. Através da análise dos dados contidos nas respostas dos órgãos, percebe-se que os órgãos governamentais estão avançando no planejamento e ações referentes à segurança da informação. Contudo o mesmo caminho não é observado quando se trata da gestão de documentos sob a perspectiva arquivística. Os resultados apontaram que a gestão da segurança da informação e a gestão documental, embora sejam complementares, não estão alinhadas quando se trata dos aspectos dos correios eletrônicos e suas características enquanto documento arquivístico dotado de autenticidade e fidedignidade, em contrapartida às práticas de seu gerenciamento, arquivamento e preservação ao longo do tempo.

Palavras- chave: Gestão de Documentos. Correio eletrônico. Segurança da Informação. Órgão público federal

ABSTRACT

Due to the appearance in the news of reports of espionage by the United States on the communications made by the Brazilian Federal Government and by those of other countries, this work aims to identify which measures are being taken by the Brazilian Federal Executive power showing the relationship between information security and communication and document management. Using the prerogatives of Access Act, questions were submitted through the Electronic Service for Information to the Citizen to a sample of seven ministries and one public company, as a means of obtaining information on government measures regarding information security in corporate electronic e-mails. Through data analysis contained in the answers of these public agencies, it is noticed that government agencies are moving forward in planning and actions related to information security. However, the same measures are not taken when it comes to document management in the archival perspective. The results show that the management of information security and document management, though complementary, are not aligned when it comes to aspects of e-mails and their characteristics as archival documents endowed with authenticity and reliability, in contrast to the practices of its management, archiving and preservation over time.

Keywords: Document management. Email. Information security. Federal government agency.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

ACMD – Administração Central do Ministério da Defesa
APF – Administração Pública Federal
ARPANET – *Advanced Research Project Agency Network*
BBN – Bolt Beranek and Newman
CONARQ – Conselho Nacional de Arquivos
CPI – Comissão Permanente de Investigação
CSIC – Comitê de Segurança da Informação e Comunicação
CTDE – Câmara Técnica de Documentos Eletrônicos
DBTA – Dicionário Brasileiro de Terminologia Arquivística
DCD – Departamento de Comunicações e Documentação
e-ARQ – Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos.
e-CFR – *Eletronic Code Federal Regulations*
e-SIC – Sistema Eletrônico de Informação ao Cidadão
EUA – Estados Unidos da América
GSI – Gabinete de Segurança Institucional
MC – Ministério das Comunicações
MCT – Ministério da Ciência, Tecnologia e Inovação
MD – Ministério da Defesa
MJ – Ministério da Justiça
MP – Ministério do Planejamento (MPOG)
MRE – Ministério das Relações Exteriores
NARA – *National Archives and Records Administration*
PoSIC – Política de Segurança da Informação e Comunicação
PR – Presidência da República
SERPRO – Serviço de Processamento
SGBD – Sistema de Gerenciamento de Banco de Dados
SIGAD – Sistema Informatizado de Gerenciamento Arquivístico
TCU - Tribunal de Contas da União
U.S. CODE - *United State Code*

SUMÁRIO

1 INTRODUÇÃO

Dois fatos envolvendo o governo norte americano desencadearam os questionamentos e a inquietação que motivaram a elaboração desta pesquisa.

O primeiro episódio, em 2013, foi a denúncia das espionagens norte-americanas direcionadas ao governo brasileiro. O segundo fato se deu em março de 2015, quando reportagens polêmicas sobre a ex-secretária de Estado dos Estados Unidos chamaram atenção na mídia internacional. As reportagens tratavam sobre o fato de que no período de 2009 a 2013, enquanto estava em exercício como secretária de Estado, Hillary Clinton, utilizou seu *e-mail* pessoal no desempenho das atividades de seu cargo, fato este que ia contra a Federal Records Act, lei federal norte-americana vigente a época, que obriga a todos os funcionários do governo federal americano a utilizar o *e-mail* corporativo (e não o *e-mail* pessoal) para tratar das questões de suas atividades laborais. Alguns dos objetivos da referida lei tratam de questões relacionadas à segurança e preservação da informação nas bases de dados do governo.

O Departamento de Estado do governo americano é o responsável pela análise dos *e-mail*s e informou[1] que por se tratar de um grande conjunto de documentos – em torno de 40.000 mil páginas de *e-mail* – o processo até a divulgação ao público demoraria algum tempo. Partidos da oposição afirmaram que Hilary expôs a segurança do Estado e que o ataque a uma representação dos EUA em Benghazi, resultou na morte de quatro pessoas, entre elas o embaixador Chris Stevens, consequência da falta de segurança nas mensagens realizadas através do *e-mail* pessoal. Hillary Clinton não foi a pioneira a quebrar as regras e fazer uso do *e-mail* pessoal nas relações governamentais, o também ex-secretário de Estado, Colin L. Powell, utilizou seu *e-mail* pessoal entre 2001 à 2005 nas atividades laborais.

[1] http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-*e-mail*-at-state-department-raises-flags.html?_r=1

Nos EUA, os agentes públicos possuem um *e-mail* oficial do governo, em especial os de alto nível da esfera federal. É por este canal que devem manter suas relações profissionais e resolver seus negócios governamentais.

Pensando nesta polêmica surgiu o questionamento sobre como são tratados os *e-mail*s no âmbito do exercício das atividades profissionais dos funcionários públicos brasileiros.

Não seria o *e-mail* enviado em função do trabalho, parte integrante de um processo laboral, um documento arquivístico e merecedor de participar das etapas de uma gestão documental?

Corroborando com as dúvidas expostas, volta a inquietar o fato de que em junho de 2013 foi descoberta a espionagem dos EUA em bases de dados do governo brasileiro, inclusive nas comunicações da presidente. Diante do exposto, surge a inquietação em saber sobre a posição do governo brasileiro a respeito do *e-mail* corporativo, em especial sobre as práticas dos servidores públicos federais, destacando aqueles de alto nível como em cargos de chefia ou políticos, que estão constantemente resolvendo os interesses do governo brasileiro, principalmente frente à esfera internacional.

Principal objetivo neste trabalho é identificar as medidas que estão sendo tomadas no governo brasileiro a respeito do correio eletrônico no decorrer das atividades de agentes públicos do poder executivo federal.

Os objetivos específicos delineados para a pesquisa foram:

a) Identificar a existência de regulamentações oficiais sobre *e-mail* corporativos na esfera do executivo nacional.

b) Analisar se órgãos do executivo federal consideram *e-mails* corporativos como documentos arquivístico.

c) Conhecer as práticas e exigências sobre os *e-mail*s corporativos no governo executivo federal.

d) Conhecer as formas de arquivamento dos *e-mail*s corporativos no executivo federal.

Pesquisa exploratória descritiva de abordagem qualitativa aplicando procedimentos de pesquisa bibliográfica e documental. Utilizou-se das prerrogativas[2] da Lei de Acesso, do qual procedeu-se o envio das perguntas pertinentes aos objetivos deste trabalho através do Serviço Eletrônico de Informação ao Cidadão (e-SIC) a uma amostra de sete ministérios e uma empresa pública. Estas perguntas buscavam informações sobre as medidas governamentais sobre a segurança da informação nos correios eletrônicos corporativos destes referidos órgãos públicos. Devido a amplitude do Poder Executivo, sendo ele dividido em ministérios, órgãos, secretarias e outras instituições, e considerando o curto período tempo para o desenvolvimento deste trabalho, foi necessário adotar a amostra citada anteriormente, inserindo na mesma, principalmente, aquelas instituições com impactos, nacionais e internacionais, na economia, desenvolvimento, segurança e defensora de direitos.

Os dados foram analisados sistematizando as repostas num quadro sinóptico. Na sequência, as informações foram confrontadas com os documentos que foram enviados como anexos às respostas e posteriormente foram ponderadas a fim de se extrair categorias que viabilizassem análises para a consecução dos objetivos específicos propostos à luz do referencial teórico.

Diante da análise dos dados e dos resultados percebe-se que os órgãos governamentais estão avançando no planejamento e ações referentes à segurança da informação, contudo o mesmo caminho não é observado quando se trata da gestão de documentos sob a perspectiva arquivística. Os resultados apontaram que embora sejam complementares, a gestão da segurança da informação e a gestão documental não estão alinhadas quando se trata dos aspectos dos correios eletrônicos e suas características enquanto documento arquivístico dotado de autenticidade, fidedignidade em contrapartida às práticas de seu gerenciamento, arquivamento e preservação ao longo do tempo.

[2] LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. Art. 10. Qualquer interessado poderá apresentar pedido de acesso a informações aos órgãos e entidades referidos no art. 1º desta Lei, por qualquer meio legítimo, devendo o pedido conter a identificação do requerente e a especificação da informação requerida.

2 CORREIO ELETRÔNICO E DOCUMENTO ARQUIVÍSTICO DIGITAL

Considerando o âmbito das atividades em que são produzidos, os *e-mail*s e documentos arquivísticos digitais possuem relações e características comuns, as quais demandam gerenciamento e tratamentos adequados a fim de cumprirem atribuições probatórias, tanto de autenticidade e fidedignidade, intrinsecamente ligadas garantindo a confiabilidade do documento, quanto para fins de sua preservação ao longo do tempo. A autenticidade é conceituada pela Câmara Técnica de Documentos Eletrônicos - CTDE (2012) como “qualidade de um documento ser exatamente aquele que foi produzido, não tendo sofrido alteração, corrompimento e adulteração”, e a fidedignidade, por sua vez, é a capacidade do documento representar os fatos que atesta. (MACNEIL, 2000, apud Rondinelli, 2004, p. 15)

2.1 Sobre o correio eletrônico

Raymond Tomlinson, considerado o inventor do *electronic mail (e-mail)*, afirma ter sido em 1971 o envio do primeiro correio eletrônico. Tomlinson conta em entrevistas realizadas por Hicks (2012) que ao criar o primeiro sistema para troca de mensagens através da rede, não tinha a intenção de mudar o mundo, pois o seu único objetivo era facilitar a comunicação com o restante da equipe que desenvolvia a rede ARPANET, sistema para o qual a empresa Bolt Beranek and Newman (BBN), em que ainda trabalha como engenheiro, fora contratada para realizar a implantação.

Poucos são os que conhecem a origem do correio eletrônico e o quanto ele evoluiu desde sua primeira aparição e muitos são os que, atualmente, possuem um *e-mail*. A grande maioria da sociedade possui pelo menos uma conta[3] de *e-mail*. O correio tradicional continua a existir, levando mensagens através de cartas, telegramas, malotes e outras espécies, porém, com a utilização do correio eletrônico, as relações se tornaram mais rápidas e econômicas, poupando tempo e dinheiro, sendo o correio eletrônico uma ferramenta muito mais eficiente que o tradicional. Junto à evolução desta ferramenta, surge uma série de questões na

[3] O termo “conta” aqui, se refere ao cadastro realizado para se obter o *e-mail*.

maneira de usá-la, especialmente quando se refere ao ambiente de trabalho e é neste âmbito que as discussões desta pesquisa estão direcionadas.

Como dito acima, o criador do *e-mail* foi Raymond Tomlinson, que, buscando uma forma ágil de comunicação com seus colegas de trabalho, acabou criando uma ferramenta de envio e recebimento de mensagens, conhecida mundialmente hoje como *e-mail*.

É recomendado no Manual de Redação (2002), ainda que indiretamente, a preferência pelo uso do correio eletrônico quando se trata das opções que eram comumente usadas como telegrama e o fax.

O Telegrama,

> Por tratar-se de forma de comunicação dispendiosa aos cofres públicos e tecnologicamente superada, deve restringir-se o uso do telegrama apenas àquelas situações que não seja possível o uso de correio eletrônico ou fax e que a urgência justifique sua utilização e, também em razão de seu custo elevado, esta forma de comunicação deve pautar-se pela concisão. (BRASIL, 2002, p.28)

O Fax *(fac-simile)*,

> é uma forma de comunicação que está sendo menos usada devido ao desenvolvimento da Internet. É utilizado para a transmissão de mensagens urgentes e para o envio antecipado de documentos, de cujo conhecimento há premência, quando não há condições de envio do documento por meio eletrônico. (BRASIL, 2002, p.29)

Assim, percebe-se que o *e-mail* é uma forma mais econômica e célere para se comunicar, sendo preciso disponibilidade de rede e acesso para conexão com o computador. No início, a capacidade do primeiro *e-mail* era pequena, não podendo realizar mensagens com muitos caracteres. Hoje temos a possibilidade de enviar *e-mails* de até 25mb, compostos de textos e anexos como fotos, vídeos e outros tipos de arquivos, além de contas capazes de armazenar gigabyte de mensagens.

Por sua abrangência e celeridade, algumas empresas e pessoas perceberam que o correio eletrônico era uma oportunidade de fazer negócios. Decorrente desta facilidade, surgiram as indesejadas mensagens *Spam*, repletas de propagandas de produtos e serviços. A ação de enviar o *Spam* para um grupo de *e-mail*s chama-se *Spamming*. Paralelamente, surgiram outras formas de mensagens abusivas. Se os *SPAMS,* por si sós, já são inconvenientes, os hackers os tornaram ainda mais

abominados, inserindo arquivos maliciosos que capturam e fornecem informações, como dados pessoais e senhas de contas bancárias e cartões de crédito.

O objetivo do correio eletrônico é proporcionar a troca de mensagens, independente da sua finalidade, seja ela pessoal ou profissional. Empresas têm adotado o *e-mail* corporativo, que, por sua vez, se estabeleceu como canal de comunicação amplamente utilizado. Os funcionários operacionalizam o envio e o recebimento de mensagens referentes às ações laborais, mantendo fluxos de comunicação interna e externa, se relacionando com fornecedores, acionistas, clientes e afins.

Entende-se por *e-mail* corporativo uma conta de correio eletrônico disponibilizada por uma organização para o uso de seus empregados. A finalidade do *e-mail* corporativo é estritamente laboral e deve ser utilizado como canal de comunicação ao que se refere à produção, tramitação e recebimento de mensagens e anexos no âmbito das atividades profissionais.

Segundo o Manual de Redação da Presidência da República (2002), o correio eletrônico se transformou na principal forma de comunicação para transmissão de documentos, pelo fato de ter baixo custo e celeridade no envio e recebimento de mensagens.

Com este pensamento, o *e-mail* corporativo deve ser inserido no processo da gestão documental. Segundo a Lei Federal nº 8.159, de 8 de Janeiro de 1991, a gestão documental é (BRASIL, 1991, pg.1) “o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente”.

O Decreto nº 8.135, de 4 de novembro de 2013, que entre outras providências dispõe sobre as comunicações de dados da administração pública federal direta que possam comprometer a segurança nacional, diz que “o armazenamento e a recuperação de dados relativos ao sistema de correio eletrônico deverão ser realizados em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal” (BRASIL, 2013, pg.1).

*E-mail*s fornecidos por órgãos e entidades da Administração Pública Federal (APF), para fins de suas atividades, podem ser considerados como e-mails corporativos. Geralmente se apresentam com layouts simples e ícones autoexplicativos, com características objetivas privilegiando as funções básicas de

enviar e receber mensagens. Embora isso não seja uma regra, e-mails corporativos costumam ter pouco espaço de armazenamento, com alguns variando de acordo com o nível hierárquico e do cargo na organização. A limitação de espaço requer dos usuários certa disciplina no uso do e-mail. O espaço reduzido leva usuários a eliminarem mensagens, de forma errônea e sem critério.

Veremos, mais adiante, como são gerenciados os correios eletrônicos corporativos e como são operacionalizados em algumas instituições federais brasileiras.

2.2 Documento Arquivístico Digital

O documento, segundo o Dicionário Brasileiro de Terminologia Arquivística (2005), é a "unidade de registro de informações, qualquer que seja o suporte ou formato", ou seja, documento pode ser entendido como toda informação registrada, não importando o suporte, embora seja esta uma definição genérica. O documento, quando produzido ou recebido por uma organização no desempenho de suas atividades, passa a ser denominado como documento arquivístico.

Contribuindo para a definição do documento arquivístico, deve-se saber que existe diferença entre documento eletrônico e documento digital, em que se encontra o seguinte silogismo: "todo documento digital é eletrônico, mas nem todo documento eletrônico é digital"[4] (CTDE). Rondinelli esclarece essa diferença, afirmando que documento eletrônico é

> o documento processado por meio eletrônico, com um formato digital. Entretanto, há outros documentos que, embora não sendo digitais, são processados eletronicamente. É o caso das fitas de áudio e videomagnéticas analógicas, que também podem ser entendidas como documentos eletrônicos. (RONDINELLI, 2005, p. 130)

O documento digital é aquele codificado em dígitos binários, somente acessível e interpretável por sistemas de computador. Segundo Innarelli (2012), o documento digital possui três elementos como sua base: o hardware (físico); o

[4] Pergunta 2. http://www.conarq.arquivonacional.gov.br/perguntas-mais-frequentes.html

software (lógico), tratando-se do aparelho e do programa responsável pela reprodução e apresentação do documento, respectivamente; e a informação.

Segundo Innarelli (2012), o documento digital possui três elementos como sua base: o hardware (físico); o software (lógico), tratando-se do aparelho e do programa responsável pela reprodução e apresentação do documento, respectivamente; e a informação (suporte + bits), referente ao armazenamento físico dos dados em suportes eletrônicos, como fitas magnéticas e discos ópticos. Innarelli (2012, p.26) afirma ainda que existem três formas dos documentos digitais serem gerados: “por meio de sistemas informatizados através de dados contidos em sistemas gerenciadores de bancos de dados (SGBD), por processo de digitalização e/ou diretamente com uso de *software* ou sistema específico”.

Para Fonseca (1998) os documentos arquivísticos são instrumentos e subprodutos das atividades institucionais e pessoais, sendo fontes primordiais de informação e prova. A autora acrescenta que para o documento arquivístico garantir seu valor probatório e testemunhal deve possuir os seguintes aspectos:

> **Autenticidade:** a autenticidade está ligada ao processo de criação, manutenção e custódia; os documentos são produto de rotinas processuais que visam ao cumprimento de determinada função, ou consecução de alguma atividade, e são autênticos quando criados e conservados de acordo com procedimentos regulares que podem ser comprovados, a partir destas rotinas estabelecidas.
> **Naturalidade:** os registros arquivísticos não são coletados artificialmente, mas acumulados de modo natural nas administrações, em função dos seus objetivos práticos; os registros arquivísticos se acumulam de maneira contínua e progressiva, como sedimentos de estratificações geológicas, e isto os dota de um elemento de coesão espontânea, embora estruturada (organicidade).
> **Inter-relacionamento:** os documentos estabelecem relações no decorrer do andamento das transações para as quais foram criados; eles estão ligados por um elo que é criado no momento em que são produzidos ou recebidos, que é determinado pela razão de sua criação e que é necessário à sua própria existência, à sua capacidade de cumprir seu objetivo, ao seu significado e sua autenticidade; os registros arquivísticos são um conjunto indivisível de relações. (FONSECA, 1998, 33-34)

Para Duranti (1998, p.9), o documento arquivístico é um documento criado ou recebido por uma pessoa física ou jurídica no curso de uma atividade prática. Para garantir a valor testemunhal, a fidedignidade e a autenticidade são fundamentais. A fidedignidade é definida como

> Capacidade de um documento arquivístico sustentar os fatos que atesta. Refere-se à autoridade e à confiabilidade de um documento. Está relacionada ao momento da produção do documento. (CTDE, 2004, p.4)

Diante de suas características e funcionalidades o documento digital requer estratégias e ações que visem sua preservação. Garantir a manutenção de sua relação orgânica, sua forma fixa e a estabilidade de seu conteúdo são primordiais para sua preservação ao longo do tempo sem que sejam comprometidos sua fidedignidade e sua autenticidade.

2.3 Correio eletrônico como documento arquivístico digital

Inúmeras instituições públicas têm buscado regulamentar o uso do correio eletrônico. Santos (2013) ressalta que um dos aspectos mais comum nesses regulamentos é a abordagem sobre o que não pode ser transmitido via sistema de correio eletrônico, isto é, atribuir responsabilidade aos usuários por suas mensagens, bem como as questões sobre vírus, spams e correntes, além da utilização do sistema exclusivamente como instrumento de trabalho. Segundo o autor, tem-se evitado abordar diretamente as questões arquivísticas, como, por exemplo, explicitar que a mensagem de correio eletrônico pode ser compreendida como um documento arquivístico.

Ponderando que mensagens de correio eletrônico são produzidas no desempenho de atividades das organizações, desta feita, o e-mail pode ser considerado documento arquivístico imbuído de valor jurídico, de prova e testemunho, sendo assim, deve ser armazenado até o momento em que esse valor prescreva.

> A indissolubilidade entre a informação, o meio documental no qual ela está vinculada, o suporte, a proveniência e, sobretudo, o vínculo entre os documentos do mesmo contexto genético, é um dos pilares da doutrina arquivística. (BELLOTTO, 2010, p.161)

Mensagens eletrônicas produzidas no âmbito das atividades desempenhadas pelos órgãos ou entidades, são documentos arquivísticos nato digitais.

Percebendo o crescimento dos correios eletrônicos nas atividades das organizações, especialmente as públicas, o Conselho Nacional de Arquivos - CONARQ, através de sua Câmara Técnica de Documentos Eletrônicos – CTDE, publicou a sua Resolução nº 36, de 19 de dezembro de 2012, que dispõe sobre "Diretrizes da Gestão do Correio Eletrônico Corporativo".

As Diretrizes para a gestão arquivística do correio eletrônico corporativo, elaborada pelo Conarq abordam sobre:

> - Mensagem de correio eletrônico como documento arquivístico.
> - Gestão arquivística de mensagem de correio eletrônico: produção, manutenção, uso e destinação.
> - Gerenciamento da mensagem de correio eletrônico dentro do Sistema Informatizado para Gestão Arquivística de Documentos – SIGAD
> - Gerenciamento da mensagem de correio eletrônico fora do SIGAD.
> - Forma documental e redação.
> - Acesso e direito de uso do correio eletrônico.
> - Preservação da mensagem de correio eletrônico.
> - Recomendações para capacitação e treinamento de usuários.

As Diretrizes orientam a gestão arquivística do *e-mail* por meio de um Sistema Informatizado de Gestão Arquivística de Documentos – SIGAD, porém a não existência dele não impede que ocorra a gestão arquivística para o correio eletrônico.

A seção 3.6 das Diretrizes, intitulada "Estratégias de apoio para gestão arquivística de mensagem de correio eletrônico na ausência de um SIGAD", aponta duas as estratégias para se obter a gestão: a "Adoção de um sistema informatizado específico para a gestão arquivística da mensagem de correio eletrônico" ou a "Gestão da mensagem de correio eletrônico dentro do próprio sistema de correio eletrônico."(CONARQ, 2012)

Na Administração Pública segue a ideia de que servidor público exerce suas atividades na legalidade e se ele decide eliminar determinado *e-mail* é por que este, realmente não possui valor algum. Este tipo de pensamento deve ser evitado por questões legais e arquivísticas. Administrar espaço de correios eletrônicos com procedimentos corriqueiros de apagar mensagens e anexos indiscriminadamente pode comprometer provas e a eliminação de documentos importantes.

Neste trabalho o *e-mail* corporativo é considerado um documento arquivístico por natureza, pois compreende-se seu papel fundamental na comunicação em meio às atividades desenvolvidas por um servidor público.

Sobre as questões de armazenamento o e-ARQ Brasil – Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos (2011) afirma que:

> A operação de arquivamento dos documentos digitais se diferencia do arquivamento dos documentos convencionais porque nestes o arquivamento é ao mesmo tempo uma operação lógica e física, como, por exemplo, arquivar um relatório na pasta Relatórios. No documento digital, como suporte e conteúdo são entidades separadas e o documento é constituído por um objeto físico (suporte), lógico (*software* e formato) e conceitual (apresentação), a operação de arquivar significa armazenar o objeto digital, mantendo sua identificação única e os ponteiros para outros objetos digitais. (CONARQ, 2011, p.29)

Obviamente que questões relacionadas ao âmbito tecnológico como hardwares e infra-estrutura de redes podem comprometer o envio, a transmissão, o recebimento, o arquivamento e arecuperção de mensagens. Contudo a atenção neste trabalho está direcionada aos aportes e recomendações técnicas que competem à Arquivística.

Para realizar o arquivamento é necessário escolher uma arquitetura do sistema de correio eletrônico que pode ser o armazenamento da mensagem no servidor, no computador do usuário cliente ou em ambos. O arquivamento deve respeitar as estratégias desenvolvidas para a preservação digital de maneira que garanta a forma fixa, ao conteúdo estável e a relação orgânica, em especial aquelas desenvolvidas pelo CONARQ.

Pensando no valor secundário dos *e-mails*, e na referência de sua função histórica e cultural, LUKESH[5] (1999, tradução nossa) afirma que “a correspondência eletrônica ou *e-mail* pessoal, quando não mantido, haverá perda significativa para a futura compreensão do trabalho dos estudiosos, para o trabalho de historiadores, e para a nossa memória coletiva.”

O arquivamento e a preservação do *e-mail* nos garantem a capacidade de:

[5] “The premise of this paper is that if electronic correspondence, personal e-mail, is not retained, there will be significant loss to future understanding of the work of today's scholars', to historians' work in general and to our collective memory.”

> - conduzir as atividades de forma transparente, possibilitando a governança e o controle social das informações;
> - apoiar e documentar a elaboração de políticas e o processo de tomada de decisão;
> - possibilitar a continuidade das atividades em caso de sinistro;
> - fornecer evidência em caso de litígio;
> - proteger os interesses do órgão ou entidade e os direitos dos funcionários e dos usuários ou clientes;
> - assegurar e documentar as atividades de pesquisa, desenvolvimento e inovação; e
> - manter a memória corporativa e coletiva. (CONARQ, 2012, p.13)

É relevante que as organizações públicas e também privadas, entendam o correio eletrônico corporativo como documento arquivístico e que se proceda às formas adequadas de sua organização, arquivamento e preservação ao longo do tempo, garantindo desta forma, a fidedignidade, o acesso e a segurança da informação.

3 SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Informação é um termo de diversos significados e que ainda não possui uma única definição aceita cientificamente.

Segundo Le Coadic,

> A informação comporta um elemento de sentido. É um significado transmitido a um ser consciente por meio de uma mensagem inscrita em um suporte espaço-temporal: impresso, sinal elétrico, onda sonora, etc. Essa inscrição é feita graças a um sistema de signos (linguagem), signo este que é um elemento da linguagem que associa um significante a um significado: signo alfabético, palavra, sinal de pontuação.
> (LE COADIC, 1996, p.5)

Le Coadic (1996) também conceitua a comunicação como um processo intermediário que permite a troca de informações entre pessoas. Enquanto a comunicação é um ato, um processo, um mecanismo, a informação é um produto, uma substancia, uma matéria. Eis que a relação entre informação e comunicação é apresentada por Saracevic (1999), onde “a informação é um fenômeno e a comunicação é o processo de transferência ou compartilhamento deste fenômeno”.

A informação é um ativo intangível de uma organização e fundamental para a tomada de decisão. Segundo a Portaria Normativa nº 1.530/MD, de 14 de maio de 2013, ativo de informação é “patrimônio composto por dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos”.

No manual “Boas práticas em segurança da informação do Tribunal de Contas da União” (TCU, 2012), explica que a segurança de informação visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. Conforme a Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, disponibilidade, integridade, confidencialidade e autenticidade podem ser entendidas da seguinte forma:

> III - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
> IV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
> V - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

> VI - 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;
> (BRASIL, 2008, p.2)

A Segurança da informação tem como função dinamizar padrões e estabelecer regras norteadoras para proteção da informação, por meio de diretrizes estabelecidas que devem prover segurança aos recursos computacionais e de informação.

Além da regulamentação de todos os aparatos legais estão, também disponíveis, normas técnicas relacionadas à gestão da segurança da informação que auxiliam as instituições a estruturarem políticas e ações de segurança da informação e comunicação. As principais normas são as da ISO/IEC série 2700, em que podem ser citadas algumas:

- ABNT NBR ISO/IEC 27001:2006/2013 - Tecnologia da informação - Técnicas de segurança - **Sistemas de gestão de segurança da informação** – Requisitos;
- ABNT NBR ISO/IEC 27002:2005/2013 - Tecnologia da informação - Técnicas de segurança - **Código de pratica para a gestão de segurança da informação;**
- ABNT NBR ISO/IEC 27004:2010 - Tecnologia da informação — Técnicas de segurança — **Gestão da segurança da informação** — Medição;
- ABNT NBR ISO/IEC 27005:2008 - Tecnologia da informação - Técnicas de segurança - **Gestão de riscos de segurança da informação;**
- ABNT NBR ISO/IEC 27011:2009 - Tecnologia da informação - Técnicas de segurança - **Diretrizes para gestão da segurança da informação para organizações de telecomunicações.**

As ações de segurança da informação envolvem levantamento de análises de riscos, princípios legais, plano de contingências. Conforme detalhado por Zanon (2014), a estrutura de segurança da informação também observa aspectos da segurança física.

> Um sistema de segurança da informação é abrangente e envolve ações de segurança operacional (por ex.: análise de riscos, normas e procedimentos, plano de contingência, etc.), segurança física (por ex.: câmeras de vídeo, alarmes, roletas, detectores de metal, etc.) e segurança lógica (detectores de cartão magnético, senhas, certificados digitais, criptografia, firewall, etc.). A política de segurança e o sistema de segurança da informação devem ser formulados em conjunto pela Administração e pelos colaboradores

> com conhecimentos específicos na área de tecnologia e segurança da informação (Zanon, 2014, p.74).

Deste modo todos os envolvidos nas atividades e processos organizacionais são responsáveis pela aplicação e permanência dos padrões de segurança adotados.

Ataques aos sistemas computacionais são vistos como problemas de vulnerabilidade. Existem várias formas de ataques e por diversos caminhos vulneráveis. Aqui, serão destacados, de acordo com a Cartilha de Segurança para Internet[6], algumas formas de eventos adversos diretamente relacionados ao correio eletrônico:

> *Spam*: é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando este tipo de mensagem possui conteúdo exclusivamente comercial também é referenciado como UCE (Unsolicited Commercial e-mail). Eles estão diretamente associados a ataques à segurança da Internet e do usuário, sendo um dos grandes responsáveis pela propagação de códigos maliciosos.
> *Falsificação de e-mail, ou e-mail spoofing*: é uma técnica que consiste em alterar campos do cabeçalho de um e-mail, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra. Como exemplo: quando alguém conhecido, solicita que você clique em um link ou execute um arquivo anexo etc.
> *Vírus*: é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. Hoje, o principal meio de propagação do vírus é o uso de pen-drives. Alguns tipos de vírus: vírus propagado por e-mail, vírus de script, vírus de macro, vírus de telefone celular.
> *Força bruta, ou brute force*: consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário. Se um atacante tiver conhecimento do seu nome de usuário e da sua senha poderá efetuar ações maliciosas como trocar a sua senha; invadir seu e-mail e seu computador, causando diversos problemas.

Na intenção de se evitar eventos suspeitos ou adversos diretamente relacionados à segurança dos sistemas ou de redes de computadores, as instituições estão cada vez mais atentas às questões que envolvem a segurança de seus ativos informacionais.

3.1 Política de Segurança da Informação e Comunicação

[6] Disponível em http://cartilha.cert.br/

A política de uma organização é fundamental para formar a cultura organizacional e é composta de normas e práticas que contribuem para a garantia de determinada conduta objetivando alcançar-se metas de comportamento ou qualidade, por exemplo. A política em questão neste trabalho é a da Segurança da Informação, que busca estabelecer práticas seguras no uso dos ativos de informação e comunicação das organizações. Segundo Marciano e Lima-Marques (2006) a política de segurança da informação deve existir em todos os setores da organização.

> Nos ambientes organizacionais, a prática voltada à preservação da segurança é orientada pelas chamadas políticas de segurança da informação, que devem abranger de forma adequada as mais variadas áreas do contexto organizacional, perpassando os recursos computacionais e de infra-estrutura e logística, além dos recursos humanos. (MARCIANO; LIMA-MARQUES, 2006)

Política de Segurança da Informação, segundo o TCU, é

> um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações.
> (TCU, 2012, p. 10)

O TCU (2012) reforça a condição da informação como ativo intangível de qualquer instituição, afirmando que aquela pode ser considerada o recurso patrimonial mais crítico, sendo importante sua segurança, pois informações adulteradas, indisponíveis ou nas mãos de pessoas de má-fé, comprometem os processos da instituição e a continuidade desta.

De acordo com Simião (2009) problemas decorrentes da falta de disponibilidade, confidencialidade, autenticidade e integridade em sistemas de informação levam à necessidade de desenvolver ações de segurança nas organizações governamentais, pois informações adulteradas, indisponíveis ou nas mãos de pessoas de má-fé, comprometem os processos da instituição e a continuidade desta.

Segundo, Zanon (2014) a política de segurança da informação consiste na formalização dos anseios da organização quanto à proteção de suas informações.

> Inicialmente deve abordar aspectos simples como identificação de usuários dos sistemas de informação, classificação das informações conforme sua prioridade, controle de acesso aos sistemas de informação, controle de uso das informações para fins institucionais, monitoramento do tráfego de informações na rede institucional, incluindo o acesso a Internet e o uso do correio eletrônico e normatização da política de segurança com aplicação de auditoria e sanções no caso de não observância da mesma. Com base em diagnósticos e análises de risco, a política deve evoluir para o estabelecimento de um sistema de segurança da informação (Zanon, 2014, p.74).

Outros instrumentos como normas internas, manuais e tutoriais podem conter detalhamentos de planos de ações de cunho prático que irão viabilizar a implantação e a manutenção da política de segurança da informação. Como, por exemplo, regras específicas para a definição de senhas nos recursos computacionais; detalhamento da política de backup, que define as regras sobre a realização de cópias de segurança dentre outras

Deste modo a política de segurança da informação e comunicação de uma instituição visa definir direitos, responsabilidades e até penalidades das partes envolvidas quanto à segurança dos ativos de informação e comunicação da empresa, importante destacar que sejam eles físicos ou digitais.

4 GESTÃO ARQUIVÍSTICA DE DOCUMENTOS DIGITAIS

A gestão de documentos é pratica integrante da Arquivologia e teve seu advento durante a Primeira Guerra Mundial devido à grande produção informacional consequente dos avanços tecnológicos, em especial, nos suportes[7] e meios de comunicação. Estes avanços tecnológicos proporcionaram a produção acelerada de documentos e informações, surgindo problemas com o gerenciamento destes.

Segundo Ribeiro (2002) como forma de solucionar os problemas gerados pela produção documental, surgiu nos Estados Unidos o conceito de *Record Management*, sendo uma nova área da gestão direcionada aos documentos, e que afirma Santos (2008), tinha a finalidade e a aplicação de métodos de economia e eficiência em documentos na fase corrente[8].

A gestão documental é definida pela Lei de Arquivos[9] (1991) como "o conjunto de procedimentos e operações técnicas referentes à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente".

A Gestão documental é aplicada somente nas fases corrente e intermediária. Estas fases, ou idades, integram o ciclo vital dos documentos, e estão intrinsecamente relacionadas aos valores primário e secundário dos documentos[10].

A fase **corrente** é a primeira fase do ciclo vital dos documentos e pela qual todo documento arquivístico terá de passar, pois é nesta fase onde ele é produzido. Os documentos da fase corrente estão sendo consultados frequentemente, são os mais próximos da atividade original deles, servem diretamente a administração. Após a fase corrente, os documentos podem ser transferidos para a fase **intermediária**, que por sua vez, é o momento em que os documentos arquivísticos deixam de ser consultados com freqüência e passam a esperar a sua destinação/eliminação ou o seu recolhimento para a ultima fase do ciclo vital, a fase permanente, onde ficam os documentos que, apesar de terem perdido seu valor

[7] Material no qual são registradas as informações. (Dicionário de Terminologia Arquivística - DBTA, 2005)

[8] Conjunto de documentos, em documentos tramitação ou tramitação não, que, pelo seu valor primário, é objeto valor primário de consultas frequentes pela entidade que o produziu, a quem compete a sua administração. (DBTA, 2005)

[9] Lei nº 8.159, de 8 de janeiro de 1991.

[10] Valor primário e secundário dos documentos é: primário - documentos que mantém importância para o setor em que foi criado. Secundário – documentos que já perderam seu valor administrativo, mas que ainda possuem valor histórico e cultural.

administrativo, primário e original, ainda são dotados de valor histórico, cultural e probatório.

Zanon (2014), ressalta que o tratamento dos documentos oficiais públicos é regido pela legislação brasileira, além de normas institucionais que, juntas, dão as diretrizes para a correta e adequada gestão documental e consequente acesso às informações a curto e longo prazo.

> Uma vez que as normas de gestão documental para a Administração Pública já existem, cabe estendê-las à gestão das informações eletrônicas por dois simples motivos: primeiro porque o tratamento da informação independe do suporte; segundo porque o gerenciamento correto das informações eletrônicas é um treinamento importante para a produção e uso de documentos digitais (Zanon, 2014, p.71).

Segundo o e-ARQ Brasil (2011), os procedimentos da gestão de documentos digitais estão baseados nas seguintes ações: captura, avaliação, temporalidade e destinação, pesquisa, localização e apresentação dos documentos, segurança, controle de acesso, trilhas de auditoria e cópias de segurança e preservação.

Com o desenvolvimento das tecnologias digitais da informação e comunicação imaginou-se que sistemas informatizados seriam capazes de prover todas as soluções para o gerenciamento da documentação digital e com isso, segundo Innarelli (2011), estaria livre de problemas tradicionais relacionados ao acondicionamento, degradação do suporte, obsolescência, falta de confiabilidade e espaço de armazenamento, porém o tempo mostrou que a tecnologia por si só não soluciona todos esses problemas, pelo contrário, cria novos problemas, os quais dependem diretamente da interferência humana e de políticas de preservação digital para serem preservados (INNARELLI, 2011, p. 82).

Questões relacionadas à obsolescência tecnológica são crucias quando o assunto é preservação ao longo do tempo. Segundo Santos (2013) a legislação nacional e as normas institucionais que tratam do objeto - documento eletrônico devem,

> objetivamente, definir o entendimento e orientar aos cidadãos e instituições públicas e privadas quanto à autenticidade e segurança contra acesso e/ou alteração não autorizados conforme se pode perceber comumente na legislação em vigor, mas também, e enfaticamente, quanto à preservação e conservação. Nesse sentido, quase nunca abrangido pela legislação, é necessário orientar as instituições sobre procedimentos que permitam confrontar e superar a obsolescência tecnológica (softwares, hardwares), visando à manutenção do acesso em longo prazo. (SANTOS, 2013, p.16)

O que se observa é que documentos digitais possuem características especiais que devem ser observadas no momento de sua preservação. A gestão de documentos digitais requer a intervenção de profissionais capacitados e técnicas arquivísticas específicas as quais oferecem organização e administração da informação e deve estar inserida na política organizacional, dessa forma, a organização terá a capacidade de:

> - conduzir as atividades de forma transparente, possibilitando a governança e o controle social das informações;
> - apoiar e documentar a elaboração de políticas e o processo de tomada de decisão;
> - possibilitar a continuidade das atividades em caso de sinistro;
> - fornecer evidência em caso de litígio;
> - proteger os interesses do órgão ou entidade e os direitos dos funcionários e dos usuários ou clientes;
> - assegurar e documentar as atividades de pesquisa, desenvolvimento e inovação, bem como a pesquisa histórica;
> - manter a memória corporativa e coletiva. (CONARQ, 2011, p.17)

As políticas de gestão das organizações influenciam diretamente nas políticas de gestão documental ou na ausência da mesma. Innarelli (2011) alerta para o fato de que as políticas de gestão visam à chamada “eficiência administrativa”, a qual acaba determinando os processos de gestão documental. A influência desse processo afeta diretamente a gestão dos documentos digitais gerados e gerenciados pelo sistema, ou seja, raramente as necessidades de gestão e preservação documental são discutidas de forma adequada e com as pessoas adequadas.

E-mails corporativos devem fazer parte não apenas das políticas de segurança da informação, mas precisam, também, receber atenção especial e serem tratados no âmbito das ações de gestão documental das organizações. Conforme delineado por leis federais mencionadas anteriormente e por normas específicas do Conselho Nacional de Arquivos. A gestão documental prevê também, para os correios eletrônicos, o gerenciamento arquivístico de seu fluxo, isto é, desde sua criação, classificação até a determinação de prazos de arquivamento, bem como os procedimentos adequados para a eliminação.

Este gerenciamento deve ser executado por sistema informatizado de gestão arquivística de documentos digitais. Este tipo de sistema é estruturado sob um conjunto de procedimentos e operações técnicas específicos para documentos digitais (natos ou não), em que obedece padrões e requisitos próprios. O modelo

brasileiro de requisitos para sistemas informatizados de gestão arquivística de documentos, denominado e-Arq Brasil pode ser usado para orientar a identificação de documentos arquivísticos digitais e estabelece requisitos mínimos para um Sistema Informatizado de Gestão Arquivística de Documentos (SIGAD), independentemente da plataforma tecnológica em que for desenvolvido e/ ou implantado. O e-arq é:

> um especificação de requisitos a serem cumpridos pela organização produtora/recebedora de documentos, pelo sistema de gestão arquivística e pelos próprios documentos, a fim de garantir sua confiabilidade e autenticidade, assim como sua acessibilidade. (e-Arq Brasil, 2009, p.9).

Os procedimentos documentais, inclusive os correios eletrônicos, devem ser contemplados pela política arquivística institucional, a qual consiste em definir ações, normas e procedimentos técnicos para a gestão e a preservação de documentos produzidos e recebidos no decorrer das atividades realizadas pelo produtor, com base na teoria e princípios da Arquivologia, ressaltando que deve haver a confluência de objetivos e alinhamento com as demais políticas institucionais.

4.1 Política de gestão documental

Política institucional de gestão documental é um instrumento normativo interno que determina, formalmente, diretrizes para que os membros desta instituição tenham conhecimento e operacionalizem a documentação de acordo com os marcos de ações estabelecidos.

Instituída a partir da cultura organizacional e estabelecida com base nos fundamentos arquivísticos, a política de gestão documental e delimitada por princípios legais (especialmente no caso dos órgãos públicos) em que implica a adoção de normas, medidas e ações práticas de cunho técnico arquivístico afim de gerenciar os conjuntos documentais de determinada instituição.

> A política pressupõe a adoção de uma série de medidas que possibilita o gerenciamento da mensagem de correio eletrônico em sua produção, uso, manutenção e destinação, aplicando as normas e os procedimentos arquivísticos para o tratamento desse documento,

> incluindo seus prazos de guarda e eliminação. (ARQUIVO NACIONAL, 2012, p.4).

A norma internacional para gestão de documentos, ISO 15.489:2001[11], destaca a relevância de se definir, nas instituições, a política de gestão documental. Segundo a Norma, as organizações devem definir e documentar as políticas de gestão de documentos a fim de garantir que seja implantada e mantida em todos os níveis da organização.

A ISO 15.489-2:2001 elucida que a política de gestão documental é uma declaração de intenções onde são expostas grandes linhas do que a instituição pretende fazer e em alguns momentos são especificados determinados planos de atuação e de procedimentos. A Norma deixa evidente que formalizar uma política não basta e oferece garantias de um gerenciamento adequado. O êxito da gestão dependerá fundamentalmente da aprovação e respaldo (visível e ativo) da direção e da disponibilidade de recursos necessários para levar a cabo sua implementação.

Santos (2013) afirma que o projeto de gestão de documentos eletrônicos vincula todas as unidades da instituição e par isso requer recursos humanos e financeiros e tem forte impacto no alcance dos objetivos de cada uma das unidades da instituição e, em consequência, da própria instituição.

> Com tal alcance horizontal e vertical na hierarquia institucional, apenas terá sucesso se for considerado pela alta gerência, diretoria ou presidência da instituição como um programa estratégico, portanto essencial ao seu futuro (SANTOS 2013, p.21).

As políticas de gestão documental podem retratar sistemas documentais híbridos, isto é, digitais e em suporte físicos, uma vez que essa tem sido uma realidade constante nas instituições.

> À instituição não interessa se a informação está registrada em documentos eletrônicos ou tradicionais, mas se ela está disponível e completa. O mundo está hoje num estado híbrido de convivência das duas tecnologias, e as informações de interesse nem sempre são encontradas em uma só dessas manifestações (SANTOS, 2013, p.21).

[11] A ISO 15.489 publicada em 2001 foi à primeira norma internacional específica à gestão de documentos está dividida em duas partes. Atualmente a gestão de documentos possui uma variedade normas ISSO e conta com a série ISO 30300

Os procedimentos documentais, inclusive os correios eletrônicos, devem ser contemplados pela política arquivística institucional, a qual consiste em definir ações, normas e procedimentos técnicos para a gestão e a preservação de documentos produzidos e recebidos no decorrer das atividades realizadas pelo produtor, com base na teoria e princípios da Arquivologia, ressaltando que deve haver a confluência de objetivos e alinhamento com as demais políticas institucionais.

De acordo com a norma ISO 15.489-2:2001, as políticas institucionais referentes à informação devem referir-se umas às outras como por exemplo, a política de TI, de gestão de documentos, de segurança da informação ou de gestão de ativos devem referenciar-se a fim de evitar ambiguidades ou sobreposição de diretivas.

> The policy statement should refer to other policesrelating to information, for example on information systems policy, information security or asset management, but should not seek to duplicate them. It should be suportes by procedures and guidelines, planning and strategy statements, disposition authorities and other documents that together make up the records management regime[12]. (ISO 15.849-2:2001).

Desta forma ressalta-se que mensagens de correio eletrônico reconhecidas como documentos arquivísticos necessitam configurarem tanto nas políticas de segurança da informação quanto na política de gestão documental, pois podem cumprir o papel de apoiar não apenas nas tarefas, funções e atividades como também servir de evidência e prova das ações da instituição.

[12] A direção da política de gestão documental deveria referir-se a outras políticas relacionadas com a informação, por exemplo, a política de sistemas de informação, de segurança da informação ou de gestão de ativos, mas sem duplica-las. Deveria estar respaldada por procedimentos e diretrizes, planos estratégicos, tabelas de temporalidade e outros documentos que, conjuntamente compõem o regime de gestão de documentos (tradução nossa).

5 O CORREIO ELETRÔNICO E A ADMINISTRAÇÃO PÚBLICA FEDERAL

5.1 Governo Brasileiro

O Governo brasileiro, com o crescente uso do correio eletrônico, tem tomado uma série de decisões, algumas isoladas e outras conjuntas, a exemplo, a Portaria Interministerial nº 141/2014, a respeito das comunicações nas atividades governamentais. Em 2013, através do site WikiLeaks[13] surgiram denuncias de que o governo dos Estados Unidos estava espionando o Brasil, especificamente a Presidente Dilma Roussef e alguns de seus ministros.

Com a repercussão da espionagem americana, a presidente determinou[14] ao Serviço Federal de Processamento de Dados (SERPRO) a implantação de um sistema que garantisse a segurança das informações de todo o governo brasileiro.

O governo tem avançado em suas normas e legislações que tratam das comunicações em meio eletrônico, entre elas estão o 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; Decreto nº 8.135, de 4 de Novembro de 2013, que dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional; e a Portaria Interministerial nº 141, de 02 de maio de 2014, entre os Ministérios do Planejamento, Orçamento e Gestão, das Comunicações e da Defesa, e que obriga a Administração Pública Federal direta, autárquica e fundacional a realizar suas comunicações por redes e serviços de tecnologia da informação por órgãos e entidades da própria Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista.

5.1.1 Serpro e Expresso V3 como medida de segurança da informação do governo brasileiro

O Serviço Federal de Processamento de Dados, o SERPRO, é uma empresa pública brasileira que funciona desde 1964 e é vinculada ao Ministério da Fazenda. O SERPRO oferece diversos serviços e entre eles está o serviço da suíte de comunicação chamada Expresso.

---

[13] https://wikileaks.org/nsa-brazil/

[14] http://g1.globo.com/politica/noticia/2013/11/dilma-assina-decreto-para-criar-sistema-de-e-mail-do-governo.html

O Expresso é uma suíte de comunicação e colaboração inteiramente desenvolvida em software livre e que no Brasil já possui algumas versões como Expresso BR e sua atual versão, o Expresso V3. Seu objetivo maior é fornecer uma ferramenta economicamente viável, com grande domínio e autossuficiência do conhecimento e difusão para corporações dentro e fora do Brasil.

A suíte Expresso originou-se do projeto alemão de software livre Tire 2.0 e já possui usuários dentro e fora do Brasil. Neste ano de 2015, se encontra na sua terceira versão, a Expresso V3, e está sendo utilizada como medida de segurança após denúncias de espionagem norte americana por alguns países, inclusive o Brasil.

Desde 2007 a SERPRO utiliza e desenvolve o Expresso, que reúne como suas principais funcionalidades:

> - Correio Eletrônico corporativo, com suporte a compar-tilhamento de pastas entre usuários;
> - Agenda pessoal e corporativa, com suporte a compartilhamento de calendários entre usuários;
> - Catálogo de endereços pessoal e corporativo;
> - Acesso a catálogos de endereços externos (em outras soluções de correio);
> - Mensagens instantâneas;
> - Boletins internos;
> - Acesso móvel;
> - Listas de distribuição de *e-mail*s;
> - Acessibilidade (por meio de aplicativos de leitura de tela e interface web do Expresso simplificada);
> - Autenticação por meio de certificados digitais; e
> - Assinatura e criptografia de *e-mail*s através de certificados digitais. (SERPRO, 2015)

O Expresso, correio eletrônico nacional, conta com comunidade ativa de especialistas das áreas públicas e privadas promovendo melhores caminhos para o projeto. O SERPRO administra e opera soluções e serviços de correio eletrônico do Microsoft Exchange, que aos poucos perde espaço para o Expresso. O Expresso vem ganhando visibilidade após o Decreto nº 8.135 de 4 de novembro de 2013, como forma de garantir soberania e segurança nacional.

A primeira meta do Expresso foi garantir utilização de certificado de sigilo, ampliar o monitoramento livre e auditável, e realizar interceptações legais, este ultimo garante o sigilo, mas repassa informações quando solicitado, ressalto ainda

que o Expresso possui criptografia, no entanto esta mesma criptografia que garante a segurança, impede a auditoria[15].

Através do Sistema de Informação ao Cidadão - e-SIC, foi informado pelo SERPRO que no Brasil, o Expresso está sendo usado nos seguintes órgãos do Governo:

> Presidência da República
> Secretaria de Portos da Presidência da República
> Secretaria de Políticas para as Mulheres da Presidência da República - SPM
> Secretaria de Políticas de Promoção da Igualdade Racial da Presidência da República - SEPPIR
> Secretaria de Aviação Civil da Presidência da República - SAC
> Ministério Planejamento Orçamento e Gestão
> Ministério das Comunicações
> Ministério das Cidades
> Ministério da Fazenda
> Ministério do Meio Ambiente
> Procuradoria Geral da Fazenda Nacional - PGFN
> Prefeitura de Valparaíso de Goiás
> Escola de Administração Fazendária - ESAF
> Autoridade Pública Olímpica - APO
> Instituto Chico Mendes - ICMBIO
> Serviço Federal de Processamento de Dados
> Conselho Administrativo de Recursos Ficais - CARF
> Engenharia, Construções e Ferrovias S.A - VALEC
> Fundo Multipatrocinado - SERPROS
> Universidade Federal do Sul da Bahia - UFSB
> Centro Federal de Educação Tecnológica Suckow da Fonseca - CEFET/RJ
> Instituto Federal de Sergipe - IFS
> Instituto Federal do Ceará – IFCE. (SERPRO, 2015)

Foram realizados workshops no intuito de criar grupos de discussão sobre temas particulares diante das dificuldades enfrentadas com: criptografia e mobilidade, segurança no desenvolvimento e homologação, arquitetura de segurança, produção e auditoria.

A suíte Expresso V3 já possui ferramentas como o Expresso Drive e o Expresso Lite. O Drive oferece serviço de nuvem que funciona como modulo de armazenamento e compartilhamento de arquivos do V3, semelhantes às aplicações do Google e Microsoft, Google Drive e Office 365, respectivamente. O Expresso

[15] O coordenador de Solução Corporativa de Comunicação e Colaboração, Marcos Melo conta que a criptografia que garante a segurança da mensagem impede que elas possam ser auditadas. http://www.serpro.gov.br/noticias/expresso-ganha-forca-no-governo-federal

Drive quando compartilha arquivos para algum outro usuário do Expresso, este arquivo pode ser editado caso possua permissão, porém, quando enviado para qualquer outro serviço de *e-mail*, este documento só poderá ser visualizado no Expresso. O Expresso Lite, por sua vez, é uma ferramenta leve para dispositivos móveis.

Como dito anteriormente, existem alguns normativos que tratam do correio eletrônico e da segurança da informação e comunicação na Administração Pública, sendo que como veremos mais a frente, os ministérios não estão seguindo em sua totalidade.

5.2 Governo Americano: uma breve contextualização

Os Estados Unidos possui uma legislação referente à administração dos seus documentos denominada de Federal Records Act, criada em 1950 e que substituiu a lei básica que existia no Código dos Estados Unidos.

Desde 1950, a Federal Records sofreu alterações até sua última emenda em 2014 pelo presidente Barak Obama passando a se chamar *Presidential and Federal Records Act Amendments of 2014*. Schellemberg (2006) conta que a lei dedicou especial atenção à administração dos documentos quando ainda nas repartições +federais e que, através da mesma, os chefes das repartições são responsáveis principalmente pelo controle eficaz da criação, manutenção e uso dos documentos nas atividades correntes.

A *Federal Records* está dividida no Título 44 – *Pubic Printing and Documents* do *United State Code* (U.S. Code) nos capítulos 21, 23,25, 27, 29, 31 e 33, estabelecendo políticas e práticas para os registros federais e instituindo o *National Archives and Records Administration* (NARA), responsável pela preservação de documentos permanentes dos EUA, semelhante ao Arquivo Nacional brasileiro.

Além do que se encontra na *U.S. Code*, atualmente, podemos encontrar no *Eletronic Code Federal Regulations* (e-CFR), no Título 36, volume 3, capítulo XII, referente à *National Archives and Records Administration*, especificamente no subcapítulo B – *Records Management*.

A *Federal Records* é aplicada em todo Estado americano, regulamentando no que tange a documentação produzida por ele, inclusive os *e-mail*s decorrentes das atividades de seus funcionários, no qual regra sobre como gerenciá-los.

6 PERCURSO METODOLÓGICO

Pesquisa exploratória descritiva de abordagem qualitativa aplicando procedimentos de pesquisa bibliográfica e documental.

Os estudos exploratórios segundo Hernandez Sapieri; Fernandes-Collado e Baptista Lucio (2006) são realizados quando o objetivo é investigar um tema ou um problema de pesquisa pouco estudado, do qual se tem muitas dúvidas ou não foi abordado antes. Desta feita a proposta de pesquisar sobre as práticas relacionadas aos correios eletrônicos em órgãos do governo federal sob a perspectiva da segurança da informação e da gestão documental se configura como um tema que suscita questionamentos pouco explorados.

A pesquisa bibliográfica é proposta neste trabalho como fundamentação teórica que orienta o princípio norteador da pesquisa motivando não apenas as bases teóricas mas, servindo também na extração de questões em que foram consideradas sob a perspectiva de ratificação ou refutação no momento da análise dos dados e na discussão dos resultados encontrados.

6.1 Coleta dos dados

Para coletar documentos e informações referentes às práticas de segurança dos *e-mail*s no âmbito das atividades do serviço público federal foram selecionados alguns órgão do executivo federal.

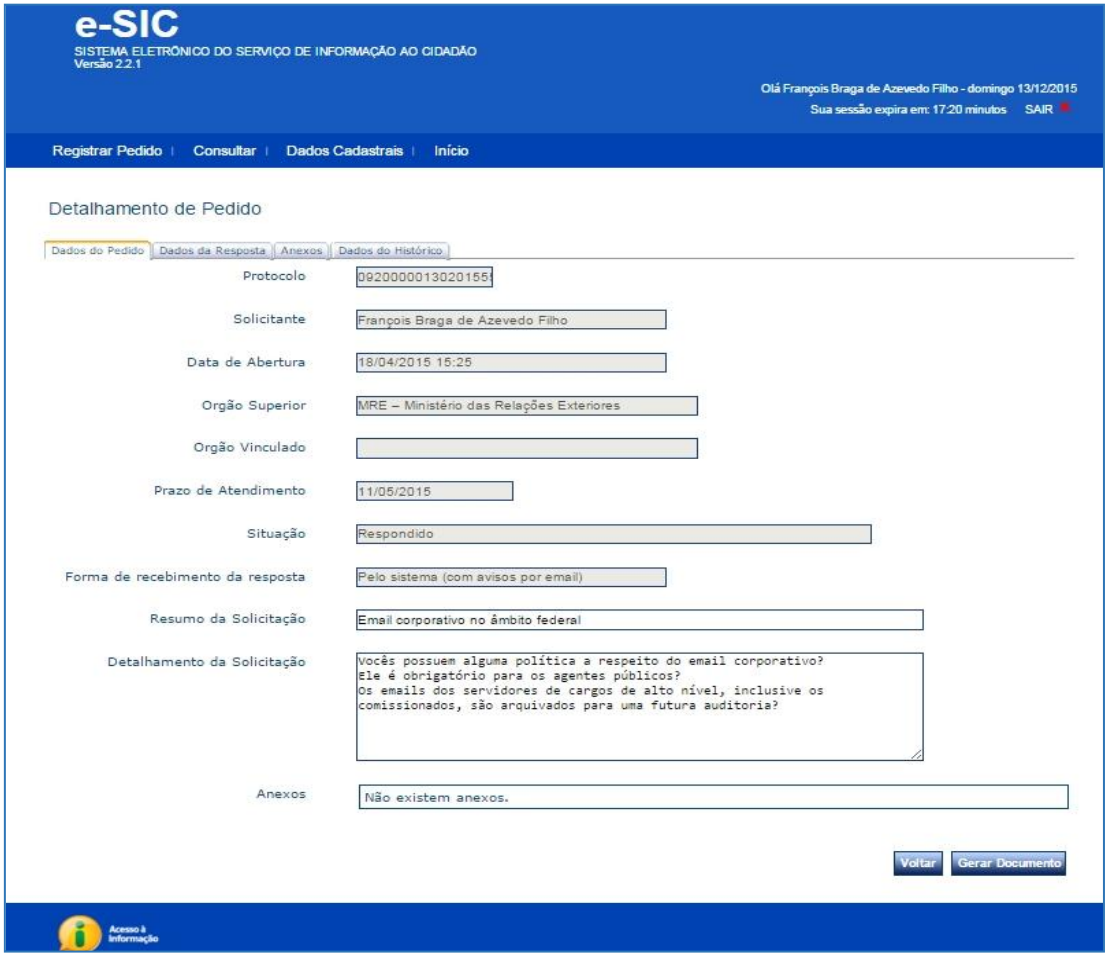
A amostra foi do tipo homogênea. Conforme explicam Hernandez Sapieri; Fernandes-Collado e Baptista Lucio (2006) a amostra homogênea ao contrário das amostras do tipo diversas possuem unidades que compartilham um mesmo perfil ou características similares. O propósito das amostras homogêneas está no centramento no tema a ser investigado ou ressaltar situações, processos ou episódios em determinado grupo social.

Dessa forma foram escolhidos sete ministérios e uma empresa pública que tratam direta ou indiretamente da economia e defesa nacional ou que mantenham relações internacionais diretas. Os órgãos selecionados foram: Ministério das Comunicações (MC), Ministério do Desenvolvimento, Indústria e Comercio Exterior (MDIC), Ministério da Ciência, Tecnologia e Inovação (MCT), Ministério da Defesa (MD), Ministério da Justiça (MJ), Ministério das Relações Exteriores (MRE), Ministério do Planejamento (MP) e para a empresa pública Serviço Federal de Processamento de Dados (SERPRO).

A coleta das informações e documentos foi realizada utilizando o recurso do Sistema Eletrônico de Serviço de Informação ao Cidadão – e-SIC. A Lei de Acesso à informação cria a em seu Art. 9, a ferramenta de Serviço de Informações ao Cidadão, onde qualquer cidadão poderá ter acesso a informações publicas, desde que preencha os dados necessários e a informação não esteja classificada como sigilosa. O órgão deverá, de preferência, responder de imediato, mas terá prazo de até 20 dias, podendo ser prorrogado por mais 10 dias desde que apresente justificativa.

Foram registrados pedidos com perguntas diretas sobre a o *e-mail* corporativo no âmbito do governo federal, conforme apresentado nas figuras 1 e 2.

Figura 1: Detalhamento dos dados do pedido de acesso à Informação: tela 1



Fonte: Sistema e-SIC

Figura 2: Detalhamento dos dados do pedido de acesso à Informação: tela 2

Caso queira outra classificação, clique no título da coluna correspondente

Ações	Protocolo	Órgão Superior	Órgão Vinculado	Data de Abertura	Prazo de Atendimento	Situação	Nome do Solicitante
Detalhar	01390000508201519	MCT – Ministério da Ciência e Tecnologia	-	18/04/2015 14:53	21/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	08850001341201598	MJ – Ministério da Justiça	-	18/04/2015 15:24	11/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	08850001342201532	MJ – Ministério da Justiça	CADE – Conselho Administrativo de Defesa Econômica	18/04/2015 15:27	11/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	09200000130201555	MRE – Ministério das Relações Exteriores	-	18/04/2015 15:25	11/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	52750000196201548	MDIC – Ministério do Desenvolvimento, Indústria e Comércio Exterior	-	18/04/2015 15:22	11/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	53850000714201568	MC – Ministério das Comunicações	-	18/04/2015 15:19	11/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	60502000831201547	MD – Ministério da Defesa	-	18/04/2015 15:20	11/05/2015	Respondido	François Braga de Azevedo Filho
Detalhar	08850002779201593	MJ – Ministério da Justiça	-	26/08/2015 15:19	15/09/2015	Respondido	François Braga de Azevedo Filho
Detalhar	08850003114201505	MJ – Ministério da Justiça	AN – Arquivo Nacional	25/09/2015 21:04	19/10/2015	Respondido	François Braga de Azevedo Filho
Detalhar	03950002087201501	MP – Ministério do Planejamento, Orçamento e Gestão	-	26/09/2015 11:59	19/10/2015	Respondido	François Braga de Azevedo Filho
Detalhar	99928000688201528	SERPRO – Serviço Federal de Processamento de Dados	-	26/09/2015 18:48	19/10/2015	Respondido	François Braga de Azevedo Filho
Detalhar	99928000689201572	SERPRO – Serviço Federal de Processamento de Dados	-	26/09/2015 18:53	19/10/2015	Respondido	François Braga de Azevedo Filho
Detalhar	53850001409201593	MC – Ministério das Comunicações	-	09/10/2015 11:20	13/11/2015	Respondido	François Braga de Azevedo Filho
Detalhar	60502001995201591	MD – Ministério da Defesa	-	09/10/2015 11:21	03/11/2015	Respondido	François Braga de Azevedo Filho
Detalhar	01390001336201509	MCT – Ministério da Ciência e Tecnologia	-	26/10/2015 16:35	26/11/2015	Respondido	François Braga de Azevedo Filho

1/2

<< Primeira | < Anterior | Próxima > | Última >> Página: Ir

Exportar Resultados

Fonte: Sistema e-SIC

O principal teor das perguntas, como pode ser observado no quadro 1, foi relacionado às práticas de segurança e gerenciamento dos *e-mail*s e foram feitas em momentos diferentes por meio de pedidos distintos no e-Sic:

Quadro 1: Perguntas solicitadas

Pergunta	Detalhamento da Solicitação:
Pergunta 1	Vocês possuem alguma política a respeito do *e-mail* corporativo? Ele é obrigatório para os agentes públicos? Os *e-mail*s dos servidores de cargos de alto nível, inclusive os comissionados, são arquivados para uma futura auditoria?

Pergunta 2	Existe algum normativo que trate sobre os *e-mail*s corporativos ou correios eletrônicos produzidos pelos servidores no desempenho de suas atividades?

Fonte: Dados da pesquisa

Na primeira solicitação de informação em abril de 2015, somente os ministérios da Justiça (Anexo A), do Desenvolvimento, Industria e Comercio Exterior (Anexo B), da Defesa (Anexo C), do Planejamento e o Serviço Federal de Processamento de Dados - Serpro (Anexo D) responderam dentro prazo de 20 dias. Todos os outros alegaram justificativas semelhantes de estarem aguardando retorno do setor responsável.

A segunda solicitação foi realizada no final de outubro de 2015 e foi enviada também ao Ministério do Planejamento, Orçamento e Gestão. Somente dois ministérios pediram prorrogação, foram eles: Ministérios da Comunicação (MC) e o de Ciência, Tecnologia e Inovação (MCT). O MC justificou a prorrogação devido a complexidade da informação (Anexo E) e o MCT (Anexo F) que estava aguardando resposta da Unidade Técnica responsável. Nesta segunda solicitação foi retornado por alguns ministérios a mesma resposta, exceto pelo ministério da Justiça e o das Relações Exteriores (Anexo G).

6.2 Análise dos Dados

Para a organização inicial das informações coletadas foi elaborado um quadro sistematizando as respostas de acordo com os órgãos respondentes, conforme apresentado nos quadros 2 e 3.

Na sequência, as respostas foram confrontadas com os documentos que foram enviados como anexos às respostas e posteriormente foram ponderadas a fim de se extrair categorias que viabilizassem análises para a consecução dos objetivos específicos propostos.

6.2.1 Sistematização e organização dos dados

Os quadros 2 e 3 apresentam, de forma sistematizada, as informações obtidas de acordo com os órgãos respondentes.

QUADRO 2: Informações coletadas e organizadas por órgão respondente – Pergunta 1

Ministério	Resposta
Ministério das Comunicações	*"Prezado(a),* *Recebemos seu Pedido de Informação nº 53850000714201568 , onde Vossa Senhoria solicita informações relacionadas a políticas sobre e-mail corporativo, nos termos: "Vocês possuem alguma política a respeito do e-mail corporativo? Ele é obrigatório para os agentes públicos? Os e-mails dos servidores de cargos de alto nível, inclusive os comissionados, são arquivados para uma futura auditoria? "* *Sobre o assunto, seguem as informações:* *1)Vocês possuem alguma política a respeito do e-mail corporativo?* *Sim, a política a respeito do uso e-mail corporativo é tratada no âmbito do Ministério das Comunicações de acordo com a Norma Operacional n° 008 de 28/11/2014 que estabelece os procedimentos para o uso de recursos de TI do Ministério e segue anexa.* *2)Ele é obrigatório para os agentes públicos?* *Sim, todos os agentes lotados no Ministério devem possuir e-mail corporativo para a comunicação dos assuntos relacionados ao trabalho.* *3) Os e-mails dos servidores de cargos de alto nível, inclusive os comissionados, são arquivados para uma futura auditoria?* *O serviço de e-mail do MC é provido pelo Serviço Federal de Processamento de Dados - Serpro, e o contrato prevê o backup das mensagens de e-mail, abrangendo todos os usuários, independente do nível hierárquico, e atende aos seguintes critérios:* *"Serviços de Backup e Restore:* *2.13.1 O backup deverá armazenar uma cópia diária das caixas postais e poderá recuperar caixas postais inteiras ou mensagens individuais de uma caixa postal;* *2.13.2 A política de backup para caixas postais deverá permitir as seguintes opções de recuperação a partir da data de solicitação (dia corrente):* *a) Caixas postais ou mensagens dos últimos 40 dias;* *b)Caixas postais ou mensagens de uma semana por mês, dos últimos doze meses;*

	c) Caixas postais ou mensagens do último dia do ano, dos últimos cinco anos; *2.13.3 A rotina de backup para os bancos de dados do correio seguro deverá permitir a seguinte opção de recuperação a partir da data de solicitação (dia corrente):* *a) Dados diários dos últimos 30 dias* *2.13.4 O backup da pasta arquivo remoto deverá guardar todas as mensagens armazenadas em qualquer período do dia, por 40 dias após a exclusão de uma mensagem. Também deverá ser possível restaurar mensagens individualmente."* *Eventuais recursos devem ser dirigidos à Secretaria-Executiva, no prazo de dez (10) dias, a contar do recebimento deste.* *O Ministério das Comunicações agradece seu contato.* *Atenciosamente,* *Subsecretaria de Planejamento, Orçamento e Administração* *Ministério das Comunicações"*
Ministério do Desenvolvimento, Industria e Comercio Exterior	*"Prezado François,* *Segue abaixo resposta da Subsecretaria de Planejamento, Orçamento e Administração - SPOA:* *"Em atenção à solicitação de Vossa Senhoria, informamos que o MDIC possui uma política de informática consolidada por intermédio da Portaria nº 12, de 24 de maio de 2006, a qual trata especificamente sobre o correio eletrônico em seu Capítulo II (segue em anexo). Esclarecemos ainda que, segundo o Art. 10 da mencionada portaria, "empregados prestadores de serviço, estagiários e bolsistas poderão, a critério do responsável pela área onde venham atuar, no interesse do serviço e durante o período de atuação no âmbito do Ministério, ter acesso ao correio eletrônico [...]". Com relação ao arquivamento dos e-mails dos servidores de cargos de alto nível, incluindo os comissionados; não há determinação prevista pela portaria de que sejam mantidos seus backups. No entanto, ressalta-se que estes backups podem ser efetuados a critério do responsável pela área de atuação destas autoridades.* *Eventual recurso deverá ser dirigido à autoridade hierarquicamente superior à que adotou a decisão, no prazo de 10 dias, contado a partir da ciência da mesma.* *Sendo o que nos competia, subscrevemo-nos"."*
Ministério da Ciência, Tecnologia e Inovação	*"Prezado Senhor François Braga de Azevedo Filho,* *Em atendimento ao Pedido de Informações nº 01390.000508/2015-19, postado no Sistema de Informações ao Cidadão, informamos a Vossa Senhoria que:* *1 – Sim. O Ministério da Ciência, Tecnologia e Inovação possui*

	política a respeito de e-mail corporativo; *2 – Sim. O uso do e-mail corporativo é obrigatório para os agentes públicos em atividade no MCTI, quando no exercício de suas funções; e* *3 – Sim. Os e-mails corporativos de todos os servidores públicos e comissionados em atividade no MCTI são arquivados para futuras auditorias.* *Atenciosamente,* *Serviço de Informações ao Cidadão - SIC* *Ministério da Ciência, Tecnologia e Inovação"*
Ministério da Defesa	*"Prezado Cidadão,* *Ao cumprimentá-lo, cordialmente, reporto-me ao pedido impetrado por Vossa Senhoria de NUP 60502.000831/2015-47, de 18 de abril de 2015.* *Em relação ao seu pedido, o Serviço de Informações ao Cidadão - SIC do Ministério da Defesa - MD encaminha, em anexo, cópia da Portaria Normativa nº 1.530/MD, de 14 de maio de 2013 que aprova a Politica de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa – ACMD. Nesta Política está previsto que o uso do e-mail na ACMD deve ser definido em norma especifica com controle de uso e cancelamento de acesso ao correio eletrônico, não sendo obrigatório o uso do e-mail pelos agentes públicos deste Ministério.* *Esclarece-se ainda, que, para todas as caixas de e-mail, são frequentemente realizadas cópias de segurança (backup).* *Nos termos do art. 21 do Decreto nº 7.724, de 16 de maio de 2012, eventual recurso sobre esta resposta deve ser dirigido à Secretária-Geral do Ministério da Defesa, no prazo de 10 dias, a contar da data desta decisão.* *Atenciosamente,* *Serviço de Informações ao Cidadão do Ministério da Defesa – SIC/MD"*
Ministério da Justiça	*"Prezado Senhor,* *Em atenção ao seu pedido de informação, registrado em 18/04/2015, encaminhamos arquivo anexo com a resposta elaborada pela Unidade competente deste Ministério.* *Registre-se que, caso julgue conveniente, poderá apresentar recurso no prazo de 10 dias, via e-SIC (www.acessoainformacao.gov.br/sistema).* *Atenciosamente,* *Coordenação do Programa de Transparência e Acesso a Informações do Ministério da Justiça* *(61) 2025-9933"*
Ministério das Relações Exteriores	*"Prezado Senhor François Braga de Azevedo Filho,* *Em atenção à solicitação protocolada pelo Serviço de Informação ao Cidadão sob o NUP nº 09200000130201555, este Ministério encaminha o documento anexo como resposta.*

	Atenciosamente, *Serviço de Informação ao Cidadão* *Ministério das Relações Exteriores"*
Serviço Federal de Processamento de Dados	*"Prezado Senhor,* *Em atenção ao seu requerimento de informação, enviado ao SIC Serpro, encaminhamos, anexo, documento normativo sobre o assunto.* *Na oportunidade esclarecemos que o Serpro não prove auditoria nos e-mail corporativo.* *Colocamo-nos à sua disposição para qualquer esclarecimento complementar.* *SIC - Serviço de Informação ao Cidadão – Serpro* *sic@serpro.gov.br (61) 20218378"*

Fonte: Dados da pesquisa

QUADRO 3: Informações coletadas e organizadas por órgão respondente – Pergunta 2

Ministério	Resposta
Ministério da Ciência, Tecnologia e Inovação	*"Prezado Senhor François Braga de Azevedo Filho,* *Em atendimento ao Pedido de Informações nº 01390.001336/2015-09, postado no Sistema de Informações ao Cidadão, informamos a Vossa Senhoria que, atualmente, este Ministério disponibiliza aos servidores, por meio da Intranet, o "Manual de Utilização dos Recursos Computacionais", aprovado pela Portaria SPOA nº 112/2005 e publicada no Boletim de Serviço Nº 15/2005, anexo, o qual define as diretrizes para a utilização do Serviço de Correio Eletrônico do Ministério.* *Adicionalmente, informamos que uma nova Norma de Criação e Utilização do Serviço de Correio Eletrônico encontra-se em elaboração e substituirá o Manual ora utilizado.* *Atenciosamente,* *Serviço de Informações ao Cidadão - SIC* *Ministério da Ciência, Tecnologia e Inovação"*
Ministério da Defesa	*"Prezado Cidadão,* *Ao cumprimentá-lo, cordialmente, reporto-me ao pedido formulado por Vossa Senhoria de NUP 60502.001995/2015-91, de 9 de outubro de 2015.* *Em relação ao seu pedido, o Serviço de Informações ao Cidadão - SIC do Ministério da Defesa - MD informa que existe atualmente a Instrução Normativa nº 3/SEORI/MD, de 22 de fevereiro de 2006 (anexa), que define os critérios para a utilização do correio eletrônico coorporativo da Administração Central do Ministério da Defesa (ACMD), visando disciplinar a troca de mensagens eletrônicas, nos âmbitos interno e externo.* *Informo, ainda que já foi validado pelo Comitê de Segurança da Informação e Comunicações (CSIC) da ACMD e está em processo de*

	aprovação uma Norma Complementar que regulamenta o subitem 5.9 da Política de Segurança da Informação e Comunicações e estabelece regras de segurança para disciplinar a utilização do serviço de correio eletrônico no âmbito da ACMD, de forma a preservar a confiabilidade, integridade, disponibilidade e autenticidade das informações por ele tramitadas. Essa Norma Complementar substituirá a Instrução Normativa nº 3/SEORI/MD. Nos termos do art. 21 do Decreto nº 7.724, de 16 de maio de 2012, eventual recurso sobre esta resposta deve ser dirigido à Secretária-Geral do Ministério da Defesa, no prazo de 10 dias, a contar da data desta decisão. *Atenciosamente,* *Serviço de Informações ao Cidadão do Ministério da Defesa – SIC/MD"*
Ministério da Justiça	*"Prezado Senhor,* *Em atenção ao seu pedido de informação, registrado em 26/10/2015, encaminhamos arquivo anexo com a resposta elaborada pela Unidade competente deste Ministério.* *Registre-se que, caso julgue conveniente, poderá apresentar recurso no prazo de 10 dias, via e-SIC (www.acessoainformacao.gov.br/sistema).* *Atenciosamente,* *Coordenação do Programa de Transparência e Acesso a Informações do Ministério da Justiça* *(61) 2025-9933"*
Ministério das Comunicações	*"Prezado Senhor,* *Trata-se de resposta ao pedido de informação protocolizado sob nº 53850001409201593, onde é solicitado se "Existe algum normativo que trate sobre os e-mail corporativos ou correios eletrônicos produzidos pelos servidores no desempenho de suas atividades."* *Em atendimento, foram anexados aos autos a Norma Operacional 08/2014 (0797674), que estabelece os procedimentos para o uso dos recursos de Tecnologia da Informação e Comunicação no âmbito do Ministério das Comunicações, e a Portaria Nº 1410/2014/SEI-MC (0797677), que trata da Politica de Segurança do Ministério em que o assunto correio eletrônico é citado na seção VI Art. 21 paragrafo 2°.* *O Ministério das Comunicações agradece o seu contato.* *Atenciosamente,* *Subsecretaria de Planejamento, Orçamento e Administração-SPOA* *Ministério das Comunicações"*
Ministério das Relações Exteriores	*"Prezado Senhor,* *Em atenção ao pedido de acesso à informação protocolado sob NUP nº 09200000667201515, encaminhamos, em anexo, arquivo com a*

	informação solicitada. *Nos termos do art. 21 do Decreto nº 7.724, de 16 de maio de 2012, eventual recurso sobre esta resposta deve ser apresentado, no prazo de 10 dias, a contar da data desta decisão."*
Ministério do Desenvolvimento, Industria e Comercio Exterior	*"Prezado François,* *Segue abaixo resposta da Subsecretaria de Planejamento, Orçamento e Administração - SPOA:* *"Em atenção à solicitação de Vossa Senhoria, informamos que o MDIC possui uma política de informática consolidada por intermédio da Portaria nº 12, de 24 de maio de 2006, a qual trata especificamente sobre o correio eletrônico em seu Capítulo II (segue em anexo).* *Eventual recurso a esta resposta deverá ser dirigido à autoridade hierarquicamente superior à que adotou a decisão, no prazo de 10 dias, contado a partir da ciência.* *Sendo o que nos competia, subscrevemo-nos".*
Ministério do Planejamento, Orçamento e Gestão	*"Senhor François,* *O Serviço de Informações ao Cidadão do Ministério do Planejamento, Orçamento e Gestão agradece o seu contato.* *Em atenção à sua solicitação, informamos que este Ministério desconhece normativo de aplicação federal ou que discipline o uso de e-mail corporativo.* *Todavia, a título de colaboração, informamos que a doutrina entende que o art. 186 da Consolidação das Leis Trabalhistas, abrangeria o e-mail corporativo como ferramenta de trabalho sujeito, portanto, a controle da empresa. Nesse sentido, o entendimento do Tribunal Superior do Trabalho em alguns casos já julgados firma-se no sentido de que não há invasão de privacidade ou violação de correspondência, quando a empresa, exercendo o poder de controle e coordenação faz o monitoramento dos conteúdos que trafegam através dos e-mails corporativos.* *Cite-se o dispositivo:* *O Ministério do Trabalho estabelecerá normas adicionais sobre proteção e medidas de segurança na operação de máquinas e equipamentos, especialmente quanto à proteção das partes móveis, distância entre estas, vias de acesso às máquinas e equipamentos de grandes dimensões, emprego de ferramentas, sua adequação e medidas de proteção exigidas quando motorizadas ou elétricas.* *Atenciosamente,* *Coordenação-geral de Aplicação das Normas* *Departamento de Normas e Procedimentos Judiciais de Pesssoal*

	Secretaria de Gestão Pública (SEGEP) *Serviço de Informações ao Cidadão (SIC)* *Ministério do Planejamento, Orçamento e Gestão (MP)* *www.planejamento.gov.br/acessoainformacao"*
Serviço Federal de Processamento de Dados	*"Prezado Senhor,* *Em atenção ao seu requerimento de informação, enviado ao SIC Serpro, encaminhamos, anexo, normativo interno que regulamenta os procedimentos sobre o uso seguro de serviços corporativos de correio eletrônico e mensageria.* *Colocamo-nos à sua disposição para qualquer esclarecimento complementar.* *SIC - Serviço de Informação ao Cidadão – Serpro* *sic@serpro.gov.br (61) 20218378"*

Fonte: Dados da pesquisa

Numa análise geral é possível identificar que não existe uma norma geral que seja obrigatória a toda Administração Pública e que trate do correio eletrônico corporativo no governo brasileiro, o que foi encontrado são políticas isoladas de cada Ministério através de instruções normativas, portarias e outros atos normativos internos.

O CONARQ já apresentou medidas de gerenciar estes *e-mail*s através da Resolução nº36, porém, apenas o Ministério da Justiça demonstrou utilizar, como podemos ver nas respostas do SIC.

O Decreto nº 8.135/12 está sendo aplicada, mas não totalmente. O sistema de correio eletrônico que atende as exigências do decreto citado é o Expresso BR, que ainda não é utilizado por toda Administração Pública.

Na inexistência de normativo específico que trate do *e-mail* corporativo, os ministérios estão adotando a Política de Segurança elaborada pelo Gabinete de Segurança Institucional como referência para criarem suas próprias políticas.

O Quadro 3 apresenta de modo resumido as principais características relacionadas ás práticas com *e-mail*s.

Com base nas respostas e anexos enviados pelos ministérios, foi possível identificar quais órgão possuem políticas que tratam do *e-mail*, se obrigatório ou não e quais possuem método de arquivamento, além de algumas observações relevantes.

QUADRO 4: principais características relacionadas ás práticas referentes a e-mails.

Ministérios	Política	Obrigato-riedade	Arquiva-mento	Observações
Ministério da Ciência, Tecnologia e Inovação.	SIM	SIM	SIM	No Manual de Utilização de Recursos Computacionais, publicado no Boletim de Serviços nº 15/05, trata do correio eletrônico na seção 6. Não foi informado sobre a forma de arquivamento.
Ministério da Comunicação	SIM	SIM	SIM	A política é através da Port. nº 1.410/2014 e da Norma Operacional nº 008/14. O arquivamento é fornecido pelo serviço do SERPRO, o mesmo que ofereço o *e-mail* corporativo. Os *e-mail* são arquivados por 5 anos.
Ministério da Defesa	SIM	NÃO	SIM	Política de Segurança da Informação e Comunicação – PoSIC/ACMD. A PoSIC foi elaborada baseada em referências legais como Lei nº 12.527/11, Dec. nº 3.505/00, Dec. nº 4.553/02 e a I.N. GSI nº 1/08.
Ministério da Justiça	SIM	NÃO	SIM*	Política de Segurança da Informação e Comunicação – PoSIC/MJ (Port. nº 3.530, de 3 de dezembro de 2013). Não possui exigência de obrigatoriedade do uso do *e-mail* na política, somente de obedecer aos procedimentos do PoSIC. Armazenamento de backups diários.
Ministério das Relações Exteriores	SIM	SIM	NÃO*	Possui Política de Segurança da Informação e Comunicação – PoSIC/ MRE e a norma especifica, Port. CSIC nº 1/15. O arquivamento fica a critério do usuário, responsável exclusivo pelo gerenciamento de sua caixa postal, pois os *e-mail*s são considerados pelo Comitê de segurança da Informação e Comunicação (CSIC) como de natureza pessoal.
Ministério do Desenvolvimento,	SIM	NÃO	NÃO	Política de Informática, cujo

Industria e Comércio Exterior				Capítulo II trata especificamente sobre o correio eletrônico. O uso do *e-mail* corporativo fica a critério do responsável da área.
Ministério do Planejamento, Orçamento e Gestão	SIM	NÃO*	SIM	Segue as orientações do Gabinete de Segurança Institucional. Não informa da obrigatoriedade do uso.
SERPRO	SIM	SIM	SIM	Norma de Segurança nº 016/12. O SERPRO utiliza seu próprio produto, o Expresso V3.

Fonte: Dados da pesquisa

7 DISCUSSÕES

Alguns ministérios afirmam que o correio corporativo é propriedade do mesmo, outros que são comunicações pessoais e pertencem ao usuário e também tem aqueles não trazem nada a respeito, ficando o correio eletrônico sem critério de arquivamento.

É importante ressaltar que o *e-mail* gerado nas atividades de um cargo carregam a bagagem informacional das relações da organização e do seu comportamento legal, sendo um documento de valor probatório e que pode vir ser de fundamental importância para garantir a probidade dos negócios governamentais.

Podemos observar através desta amostra de ministérios que de 2012 à 2015 tem crescido e sofrido reformas o número de normativos internos referentes aos correios eletrônicos, porém ainda não existe uma norma federal a respeito deste tema.

Ao contrário da Federal Records, as regulamentações brasileiras desenvolvidas até o momento são apenas políticas de governo, ou seja, são medidas criadas como exemplo do que seria o ideal, que por sua vez não tem uma obrigatoriedade, fica a critério da Administração Pública (APF) adotar ou não, enquanto as políticas de Estado como a Federal Records obrigam toda a Administração a seguir àquelas medidas.

Diante do exposto é pertinente comentar a respeito do documento “Estratégia de Segurança da Informação e comunicação e de segurança cibernética da administração federal da administração pública federal” elaborado pelo Gabinete de Segurança Institucional da Presidência da República em 2015 e que complementa o Normativo GSI nº 01/08. O documento reúne metas e objetivos para serem atingidos até 2018, buscando a segurança dos setores de Informação e Comunicação e da Cibernética no âmbito da APF, contribuindo desta forma com a segurança institucional e a soberania nacional. Nos marcos de 2014 apresentados no documento das estratégias está o Relatório Final da CPI da Espionagem, elaborado pela Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, denuncia esta citada neste trabalho, onde foi estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar *e-mail*s, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas. Como parte da estratégia de segurança da informação e

segurança cibernética para os anos de 2015 - 2018 estão as seguintes medidas e recomendações:

> - Elaboração de uma Estratégia Nacional de Segurança Cibernética, realçando que houve unanimidade entre os convidados à CPI, de que mais urgente do que a Estratégia, é que sejam delineadas as principais medidas de segurança cibernética para o Estado brasileiro, englobando ações coordenadas entre os setores público e privado.
> - Criação de uma agência para a segurança cibernética no âmbito da Administração Pública Federal, favorecendo visão de conjunto no tema e ações mais eficazes e efetivas. Alternativamente à criação de um novo órgão, poderia ser alterada a estrutura de órgão já existente, modificando suas atribuições, para lhe conferir capacidade de atuar, com independência, em sua totalidade e em estreita coordenação com os demais órgãos atuantes nos mais diversos temas que englobam a segurança cibernética.
> (GSI/PR, 2015, 32-33)

Dos normativos apresentados na pesquisa, o mais antigo é do Ministério de Ciência, Tecnologia e Inovação (MCT), o “Manual de Utilização dos Recursos Computacionais” publicado no Boletim de serviço nº 15 de 2005. O MCT informou em sua segunda resposta que está sendo elaborada a uma nova “Norma de Criação e Utilização do Serviço de Correio Eletrônico”, assim como o Ministério da Defesa, que irá substituir a Instrução Normativa nº 3/2006 por uma Norma Complementar, que como disseram em sua segunda resposta, “já foi validado pelo Comitê de Segurança da Informação e Comunicações (CSIC) da Administração Central do Ministério da Defesa (ACMD) e está em processo de aprovação”.

Alguns ministérios como o da Comunicação, Justiça e Relações Exteriores elaboraram recentemente seus normativos. O MC possui o Normativo Operacional nº 008 e a Port. nº 1.410, ambas de 2014; o MJ criou uma política de segurança da informação e comunicação em 2012 e alterou a mesma em 2013; e o MRE, em sua primeira resposta informou que a Norma DCD nº 1/2006 seria substituída em breve por um normativo que o Comitê de Segurança da informação e Comunicação, instituído pela PoSIC, estava elaborando sobre o correio eletrônico corporativo e logo em sua segunda resposta, já enviou o novo normativo, a Portaria CSIC nº 1, de 19 de Junho de 2015.

O fato dos ministérios estarem criando normativos tratando da SIC nestes últimos anos significa que a segurança da informação está chamando a atenção dos órgãos poder executivo e considerando

Diante das análises, observa-se que há prevalência de atenção na Segurança da Informação em detrimento da falta de menção à gestão documental.

Conforme dispõe a Lei 8.159/199 a gestão documental é dever do Poder Público, é instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elementos de prova. Embora regida pela Lei e pelo decreto 4.073/2002 dentre outros instrumentos normativos, a gestão documental ainda é periférica e carece ser compreendida em suas funcionalidades e como determina a legislação. Segundo Indolfo (2013) o desconhecimento e a não implementação de ações arquivísticas nos órgãos públicos traz consequências de ineficiência na operacionalização de serviços públicos afetando, também o acesso à informação.

> A ausência de formulação e implementação de políticas arquivísticas que visem à implantação de programas de gestão de documentos nos órgãos e entidades do Poder Executivo Federal afeta diretamente o acesso à informação governamental disponível ao próprio Estado e aos cidadãos (INDOLFO, 2013, p. 4).

Diante das características das políticas de segurança da informação e da gestão documental é possível perceber que ambas, de forma geral, são elementos componentes da gestão da informação e se complementam.

Entretanto, a exemplo da forma em que são arquivados os e-mails corporativos, não se observa o diálogo entre as políticas de segurança da informação com a gestão documental. O intercâmbio destas ações complementares de gestão são cruciais aos órgãos públicos, principalmente por questões de transparência, segurança, acesso e preservação da informação.

8 CONSIDERAÇÕES FINAIS

Como visto no decorrer do trabalho está é mais uma pauta a ser discutida no desenvolvimento de políticas Arquivísticas, mas além de arquivística, na formação de uma política de Estado que busca diminuir os crimes governamentais através da transparência de suas relações e no combate de intervenções estrangeiras com a criação de dispositivos ligados a segurança da informação e comunicação.

O pouco referencial teórico encontrado além de ter dificultado o desenvolvimento do trabalho, mostrando que ainda é pequeno o número de pesquisas na área da segurança da informação na perspectiva da arquivologia.

Algo interessante de se ressaltar é a frequência que o termo backup, referente ao arquivamento dos correios eletrônicos, apareceu nos normativos.

Segundo o e-Arq (2011), o backup é a realização de cópias periódicas com o propósito de restaurações futuras em casos de falha de software, hardware ou acidentes, enquanto o arquivamento vai além e possui uma outra finalidade. O arquivamento busca para o documento eletrônico, assim como para os convencionais, controlar os títulos das pastas ou diretórios nos repositórios digitais no qual serão arquivados, sendo uma operação lógica e física. O backup é uma medida simples e não deve ser confundida com a complexidade do arquivamento. Enquanto o backup é unicamente uma cópia de segurança, o arquivamento é composto por uma série de etapas como inspeção, analise ordenação e o próprio arquivamento, é ao mesmo tempo um processo lógico e físico. A Resolução nº 43 do CONARQ (2015) diz que a gestão de documentos digitais deve ser feita com a utilização de Repositórios Arquivísticos Digitais Confiáveis – RDC-Arq, para que a cadeia de custódia não seja quebrada, garantindo autenticidade e preservação dos documentos.

Cabe nesta conclusão as palavras de Simião (2009), que

> vale expressar a certeza quanto a utilidade do novo conceito de SIC, explorado neste trabalho, para as organizações governamentais, especialmente para aquelas comprometidas com a eficácia do serviço público e que pautam suas ações em princípios democráticos em prol de uma sociedade cada vez mais justa. A segurança da informação e comunicações, antes de ser um conceito, é uma questão de atitude ética, legal, discreta, honesta e, acima de tudo, deve ser um hábito natural em nossas vidas. (SIMIÃO, 2009, p. 71)

REFERÊNCIAS

BRASIL. Conselho Nacional de Arquivos. Câmara Técnica de Documentos Eletrônicos. **e-ARQ Brasil: Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos / Câmara Técnica de Documentos Eletrônicos**. 1.1. versão. - Rio de Janeiro : Arquivo Nacional, 2011. 136 p.

_____. Conselho Nacional de Arquivos. Perguntas mais frequentes. **Câmara Técnica de Documentos Eletrônicos**. Disponível em: < http://www.conarq.arquivonacional.gov.br/perguntas-mais-frequentes.html>. Acesso em: 01 nov. 15.

_____. Conselho Nacional de Arquivos. **Classificação, temporalidade e destinação de documentos de arquivo; relativos às atividades-meio da administração pública/ Arquivo Nacional.** Rio de Janeiro: Arquivo Nacional, 2001. p. 156

_____. Conselho Nacional de Arquivos. **Dicionário brasileiro de terminologia arquivística**. Rio de Janeiro: Arquivo Nacional, 2005. 232p

_____. 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.

_____. Conselho Nacional de Arquivos. **RESOLUÇÃO Nº 43, DE 04 DE SETEMBRO DE 2015.** Altera a redação da Resolução do CONARQ nº 39, de 29 de abril de 2014, que estabelece diretrizes para a implementação de repositórios digitais confiáveis para a transferência e recolhimento de documentos arquivísticos digitais para instituições arquivísticas dos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR.

BELLOTTO, Heloisa Liberalli. Da gênese à função: o documento de arquivo como informação e testemunho. In.: FREITAS, Ligia Silva de; MARCONDES, Carlos Henrique; RODRIGUES, Ana Célia (Orgs.). **Documento: Genese e contextos de uso.** Niteroi: EdUFF, 2010, p. 161-174.

BRASIL. DECRETO Nº 8.135, DE 4 DE NOVEMBRO DE 2013. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. **Diário Oficial [da República Federativa do Brasil]**, Brasília, DF, 05 de nov. 2013, P. 2.

_____. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências. **Diário Oficial [da República Federativa do Brasil]**, Brasília, DF, 09 de jan. 1991, P. 455.

_____. Decreto nº 3.505, de 13 de Junho de 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública. **Diário Oficial [da República Federativa do Brasil]**, Brasília, DF,

_____. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011. 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. **Diário Oficial [da República Federativa do Brasil]**, Brasília, DF, 18 de Nov. 2011, P. 1.

_____. Portaria Interministerial MP/MC/MD Nº 141 DE 02/05/2014. Dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria. **Diário Oficial [da República Federativa do Brasil]**, Brasília, DF, 5 mai 2014.

_____. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0** / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República, 2015.

_____. Presidência da República. Manual de redação da Presidência da República / Gilmar Ferreira Mendes e Nestor José Forster Júnior. – 2. ed. rev. e atual. – Brasília : Presidência da República, 2002..

_____. Portaria Normativa nº 1.530/MD, de 14 de maio de 2013. Aprova a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa e dá outras providências. **Diário Oficial [da República Federativa do Brasil]**, Brasília, DF, 16 de mai. 2013. p.33.

DURANTI, Luciana. ***Diplomatics: new uses for an Old Science. Society of American Archivists.*** Maryland, 1998.

ESTADOS UNIDOS DA AMERICA. Federal Records Act. 1950 Disponível em: https://www.law.cornell.edu/uscode/text/44/chapter-31 Acesso em: 01 nov. 15.

FONSECA, Maria Odila. Informação, arquivos e instituições arquivísticas**. Arquivo & Administração**. Rio de Janeiro, v. 1, n. 1, p. 33-44, jan./jun. 1998.

HERNANDEZ SAPIERI, Roberto; FERNANDES-COLLADO, Carlos; BAPTISTA LUCIO, Pilar. Metodologia de la investigación. 4. ed. México: McGraw-Hill Interamericana. 2006.

INDOLFO, Ana Celeste. Dimensões político-arquivísticas da avaliação de documentos na administração pública federal (2004-2012). In: Encontro Nacional de Pesquisa em Ciência da Informação, 14, ENANCIB. 2013.

INNARELLI, Humberto Celeste. Preservação digital e seus dez mandamentos. In: SANTOS, Vanderlei Batista; INNARELLI, Humberto Celeste; SOUSA, Renato Tarciso Barbosa de (Org.). **Arquivística: temas contemporâneos, classificação,**

preservação digital, gestão do conhecimento. 3ª Ed:Distrito Federal: SENAC, 2012. 224p.

INNARELLI, Humberto Celeste. Preservação digital: a influência da gestão dos documentos digitais na preservação da informação e da cultura. **Revista Digital de Biblioteconomia e Ciência da Informação, Campinas**, *v.8, n. 2, p. 72-87, jan./jun. 2011*.

ISO 15.489-2. Records management – part 2: guidelines. Geneva, ISO, 2001. 39p.

HICKS, Jesse. **Ray Tomlinson, the inventor of *e-mail*: 'I see *e-mail* being used, by and large, exactly the way I envisioned'.** The Verge. Disponível em: http://www.theverge.com/2012/5/2/2991486/ray-tomlinson-*e-mail*-inventor-interview-i-see-*e-mail*-being-used Acesso em: 01 nov. 15.

LE COADIC, Yves-François. A ciência da informação. Brasília: Briquet de Lemos, 1996.

LUKESH, Susan S. *E-mail* and Potential Loss to Future Archives and Scholarship or The Dog that Didn't Bark. First Monday, v. 4, n.9. September 6th 1999. Disponível em: < http://www.firstmonday.org/ojs/index.php/fm/article/view/692/602 > . Acesso em: 01 nov. 15.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. O enfoque social da segurança da informação. Ci. Inf., Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006.

Mary Bellis. **History of *E-mail* & Ray Tomlinson.** About.com Disponível em: http://inventors.about.com/od/estartinventions/a/*e-mail*.htm Acesso em: 01 nov. 15.

MICHAEL S. SCHMIDT. **Hillary Clinton Used Personal *E-mail* Account at State Dept., Possibly Breaking Rules.** The New York Times. Disponível em: http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-*e-mail*-at-state-department-raises-flags.html?_r=1 Acesso em: 01 nov. 15.

Paulo Heitlinger. ***E-mail*.** Disponível em: http://www.tipografos.net/internet/*e-mail*.html Acesso em: 01 nov. 15.

Ray Tomlinson. **The First Network *E-mail*.** Disponível em: http://openmap.bbn.com/~tomlinso/ray/firste-*mail*frame.html Acesso em: 01 nov. 15.

RONDINELLI, Rosely Curi. **Gerenciamento arquivístico de documentos eletrônicos: uma abordagem teórica da diplomática arquivística contemporânea** / Rosely Curi Rondinelli. 4. Ed. Rio de Janeiro: Editora FGV, 2005. 160p.

SANTOS, Vanderlei Batista dos. Gestão de documentos arquivísticos eletrônicos: o caminho percorrido pela administração pública brasileira. **Cadernos de História**, Belo Horizonte, v. 14, n. 20, p.9-31, 2013.

SARACEVIC, T. Information science. **Journal of the American Society for Information Science**, v. 50, n. 12, p. 1051–1063, Oct. 1999.

SIMIÃO, Reinaldo Silva. **Segurança da Informação e Comunicações:** conceito aplicável em organizações governamentais**.** Brasília, Junho/2009

SCHELLEMBERG, T.R.. **Arquivos Modernos.** FGV, 6ª edição, 2006.

SERPRO. **Notícias.** 2015. Disponível em: http://www.serpro.gov.br/noticias Acesso em: 01 nov. 15.

Brasil. Tribunal de Contas da União. **Boas práticas em segurança da informação** / Tribunal de Contas da União. – 4. ed. – Brasília : TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012. 103 p.

ZANON, Sandra Buth. Gestão e segurança da informação eletrônica: Exigências para uma gestão documental eficaz no Brasil. **Biblios.** n.56, 2014, p.69-70.

Anexos

Anexo A: Documentos enviados como anexo pelo Ministério da Justiça

Anexo B: Documentos enviados como anexo pelo Ministério do Desenvolvimento Indústria e Comércio Exterior

Anexo C: Documentos enviados como anexo pelo Ministério da Defesa

Anexo D: Documentos enviados como anexo pelo Serpro

Anexo E: Documentos enviados como anexo pelo Ministério da Comunicação

Anexo F: Documentos enviados como anexo pelo Ministério da Ciência e Tecnologia

Anexo G: Documentos enviados como anexo pelo Ministério das Relações Exteriores

Anexo A

Documentos enviados como anexo pelo Ministério da Justiça

0492125 08850001341201598

MINISTÉRIO DA JUSTIÇA

Esplanada dos Ministérios Bloco T, Ed. Sede - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: 2025*3063/6942 e Fax: 2025*3000 - www.justica.gov.br

Ofício nº 70/2015/SIC SE/SE-MJ

Brasília, 11 de maio de 2015.

Ao Senhor François Braga de Azevedo Filho

Assunto: Lei de Acesso à Informação – VOCÊS POSSUEM ALGUMA POLÍTICA A RESPEITO DO EMAIL CORPORATIVO? ELE É OBRIGATÓRIO PARA OS AGENTES PÚBLICOS? OS EMAILS DOS SERVIDORES DE CARGOS DE ALTO NÍVEL, INCLUSIVE OS COMISSIONADOS, SÃO ARQUIVADOS PARA UMA FUTURA AUDITORIA? - **SIC/MJ Nº 08850.001341/2015-98.**

Prezado Senhor,

Reporto-me à Solicitação de Informação – SIC/MJ nº 08850.001341/2015-98, encaminhada por Vossa Senhoria em 18 de abril de 2015 ao SIC CENTRAL MJ, para, nos termos da manifestação da Coordenação-Geral de Tecnologia da Informação – CGTI/SE/MJ, encaminhar cópia do Despacho nº 401/2015/DIARTI/CGTI/SPOA/SE (0424180), de 27 de abril de 2015.

Atenciosamente,

EDUARDO SPANÓ JUNQUEIRA DE PAIVA
Ponto Focal da Secretaria Executiva

Documento assinado eletronicamente por **EDUARDO SPANO JUNQUEIRA DE PAIVA**, **Ponto Focal do SIC SE**, em 11/05/2015, às 19:21, conforme o § 1° do art. 10 da Medida Provisória nº 2.200/01.
N° de Série do Certificado: 1231720

0424180 08850001341201598

MINISTÉRIO DA JUSTIÇA

Despacho nº 401/2015/DIARTI/CGTI/SPOA/SE

Em, 27 de abril de 2015.

Assunto: **Lei de Acesso à Informação**
Destino: **Coordenação-Geral de Tecnologia da Informação**
Processo: **08850001341201598**

1. Em atenção ao **Despacho n° 54/2015/SIC SE/SE**, informamos que o Ministério da Justiça possui a Política de e-mail corporativo, a qual é tratada no âmbito de Política de Segurança da Informação e Comunicações do Ministério da Justiça.

2. É obrigatório a todos os agentes públicos obedecerem a Política de Segurança da Informação e Comunicações.

3. Todas as caixas de e-mail do Ministério da Justiça possuem cópia de segurança (backup), inclusive os e-mails dos cargos de alto nível e os comissionados.

Respeitosamente,

Documento assinado eletronicamente por **DANIELA CRISTINA PORTO**, **Analista Técnico-Administrativo - ATA**, em 29/04/2015, às 11:32, conforme o § 2° do art. 10 da Medida Provisória n° 2.200/01.

Documento assinado eletronicamente por **LEO ROSSATO BISCAGLIA**, **Chefe da Divisão de Administração de Recursos de Tecnologia da Informação**, em 30/04/2015, às 12:29, conforme o § 2° do art. 10 da Medida Provisória n° 2.200/01.

A autenticidade do documento pode ser conferida no site http://sei.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0424180** e o código CRC **86428ACA**.

PORTARIA Nº 3.240, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando os resultados dos julgamentos proferidos pela Comissão de Anistia, na 61ª Sessão de Turma, realizada no dia 19 de agosto de 2009, e na 14ª Sessão Plenária, realizada no dia 17 de outubro de 2012, no Requerimento de Anistia nº 2002.01.11667, resolve:

Ratificar a condição de anistiado político de SEBASTIÃO PALMEIRA CORRÊA, portador do CPF nº 298.087.667-49, e conceder contagem de tempo, para todos os efeitos, do período compreendido de 17.12.1987 a 05.10.1988, nos termos do artigo 1º, incisos I e III da Lei n.º 10.559, de 13 de novembro de 2002.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.241, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 12ª Sessão de Turma, realizada no dia 19 de julho de 2012, no Requerimento de Anistia nº 2002.01.11631, resolve:

Indeferir o Requerimento de Anistia formulado por PAULO RENATO PINTO FERREIRA, portador do CPF nº 346.791.707-00.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.242, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 7ª Sessão Plenária, realizada no dia 24 de maio de 2012, no Requerimento de Anistia nº 2002.01.11340, resolve:

Declarar anistiada política MARIA LÚCIA RIBEIRO MARTINS, portadora do CPF nº 126.965.107-25, e conceder a reparação econômica, de caráter indenizatório, em prestação única, no valor de R$ 100.000,00 (cem mil reais), nos termos do artigo 1º, incisos I e II c/c artigo 4º, §§ 1º e 2º, da Lei n.º 10.559, de 13 de novembro de 2002.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.243, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 13ª Sessão Plenária, realizada no dia 19 de setembro de 2012, no Requerimento de Anistia nº 2002.01.10284, resolve:

Indeferir o Requerimento de Anistia formulado por FRANCISCO ASSIS DE LIMA, portador do CPF nº 004.360.381-53.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.244, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 13ª Sessão de Turma, realizada no dia 22 de agosto de 2012, no Requerimento de Anistia nº 2002.01.09082, resolve:

Indeferir o Requerimento de Anistia "post mortem" de AMPELIO TRIZOTO, filho de LUIZA BURTET, formulado por VILSON TRIZOTTO, portador do CPF nº 060.184.679-68.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.245, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 14ª Sessão Plenária, realizada no dia 17 de outubro de 2012, no Requerimento de Anistia nº 2002.01.09046, resolve:

Indeferir o Requerimento de Anistia "post mortem" de ARLINDO LEITE DE SIQUEIRA, filho de JOSEFA ALVES DE SIQUEIRA, formulado por MARIA HELENA DUARTE DE SIQUEIRA, portadora do CPF nº 327.839.574-34.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.246, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 13ª Sessão Plenária, realizada no dia 19 de setembro de 2012, no Requerimento de Anistia nº. 2002.01.07693, resolve:

Ratificar a condição de anistiado político "post mortem" de NELSON BARBOSA, filho de MARIA DA CONCEIÇÃO BARBOSA, e conceder a NAZIRIA MARQUES BARBOSA, portadora do CPF n.º 048.263.737-40, a substituição da pensão por morte de anistiado político, nos mesmos valores que vem percebendo do INSS, sob NB 59/046.826.580-5, pelo regime de reparação econômica, de caráter indenizatório, em prestação mensal, permanente e continuada, sem efeitos financeiros retroativos, nos termos do artigo 1º, incisos I e II c/c artigo 19 da Lei nº 10.559, de 13 de novembro de 2002.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.247, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 3ª Sessão Plenária, realizada no dia 22 de março de 2012, e o Despacho da Vice-Presidente da Comissão de Anistia, datado de 27 de setembro de 2012, no Requerimento de Anistia nº 2001.01.04335, resolve:

Retificar a Portaria Ministerial n.º 1.657 de 07 de agosto de 2012, publicada no Diário Oficial da União de 08 de agosto de 2012, para ratificar a condição de anistiado político de ALTAMIR GONÇALVES PETTERSEN, portador do CPF nº 173.731.077-53, conceder reparação econômica, de caráter indenizatório, em prestação mensal, permanente e continuada, no valor de R$ 2.000,00 (dois mil reais), com efeitos financeiros retroativos da data do julgamento em 22.03.2012 a 05.10.1988, perfazendo um total retroativo de R$ 610.133,33 (seiscentos e dez mil, cento e trinta e três reais e trinta e três centavos), nos termos do artigo 1º, incisos I e II da Lei n.º 10.559, de 13 de novembro de 2002.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.248, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 12ª Sessão Plenária, realizada no dia 05 de setembro de 2012, no Requerimento de Anistia nº 2001.02.00923, resolve:

Declarar anistiado político ANIZIO RODRIGUES DA SILVA, portador do CPF nº 286.382.129-68, conceder reparação econômica, de caráter indenizatório, em prestação mensal, permanente e continuada, no valor de R$ 1.299,00 (um mil, duzentos e noventa e nove reais), com efeitos financeiros retroativos da data do julgamento em 05.09.2012 a 13.01.1993, perfazendo um total retroativo de R$ 331.807,90 (trezentos e trinta e um mil, oitocentos e sete reais e noventa centavos), e contagem de tempo, para todos os efeitos, do período compreendido de 25.04.1985 a 05.10.1988, nos termos do artigo 1º, incisos I, II e III da Lei nº 10.559, de 13 de novembro de 2002.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.249, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 13ª Sessão Plenária, realizada no dia 19 de setembro de 2012, no Requerimento de Anistia nº 2003.01.22864, resolve:

Indeferir o Requerimento de Anistia formulado por MÁRCIO ROBERTO ALELUIA, portador do CPF nº 155.379.786-87.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.250, DE 19 DE DEZEMBRO DE 2012

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais, com fulcro no artigo 10 da Lei nº 10.559, de 13 de novembro de 2002, publicada no Diário Oficial de 14 de novembro de 2002 e considerando o resultado do julgamento proferido pela Comissão de Anistia, na 20ª Sessão de Turma, realizada no dia 20 de setembro de 2012, no Requerimento de Anistia nº 2006.01.53633, resolve:

Declarar anistiado político VICENTE CELSO QUAGLIA, portador do CPF nº 032.271.628-49, e conceder reparação econômica, de caráter indenizatório, em prestação única, no valor correspondente a 30 (trinta) salários mínimos, equivalente nesta data a R$ 18.660,00 (dezoito mil, seiscentos e sessenta reais), nos termos do artigo 1º, incisos I e II c/c artigo 4º, § 1º, da Lei n.º 10.559, de 13 de novembro de 2002.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.251, DE 19 DE DEZEMBRO DE 2012

Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça, e dá outras providências.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso das atribuições que lhe conferem o art. 87, parágrafo único, inciso II, da Constituição, e o Decreto nº 6.061, de 15 de março de 2007, e tendo em vista o disposto no Decreto nº 3.505, de 13 de junho de 2000, e na Norma Complementar nº 3, de 30 de junho de 2009, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicações do Ministério da Justiça - POSIC/MJ.

Art. 2º A POSIC/MJ aplica-se a todos os órgãos e entidades da estrutura organizacional do Ministério da Justiça.

Parágrafo único. Os órgãos e entidades de que trata o caput poderão elaborar políticas setoriais de segurança da informação e comunicações, desde que observados os princípios e as diretrizes gerais da POSIC/MJ.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 3º A Política de Segurança da Informação e Comunicações do Ministério da Justiça - POSIC/MJ objetiva dotar os órgãos e entidades da estrutura organizacional do Ministério de princípios, diretrizes, critérios e instrumentos aptos a assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, protegendo-os contra ameaças e vulnerabilidades.

Art. 4º Para efeitos da POSIC/MJ, considera-se:

I - agente público: 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 no Ministério;

II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que possa resultar em dano para um sistema, órgão ou entidade da estrutura organizacional do Ministério;

III - ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - 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;

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

VI - continuidade de serviços: capacidade estratégica e tática de um órgão ou entidade da estrutura organizacional do Ministério de se planejar e responder a incidentes e interrupções de funcionamento, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

VII - disponibilidade: propriedade de que a informação esteja acessível e seja utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

VIII - 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 e de implementar a segurança da informação e comunicações no Ministério;

IX - gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para um órgão ou entidade da estrutura organizacional do Ministério e os possíveis impactos no funcionamento de seus serviços e atividades, caso essas ameaças se concretizem;

X - 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 ativos de informação, permitindo equilibrá-los com os custos operacionais e financeiros envolvidos;

XI - incidente de segurança: qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas de computação ou redes de computadores;

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

XIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIV - Segurança da Informação e Comunicações - SIC: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XV - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; e

XVI - vulnerabilidade: conjunto de fatores internos ou causas potenciais de um incidente de segurança que pode ser evitado por uma ação de SIC.

Nº 245, quinta-feira, 20 de dezembro de 2012 Diário Oficial da União - Seção 1 ISSN 1677-7042 119

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 sítio 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 sítio 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.

1411504 08850003463201519

MINISTÉRIO DA JUSTIÇA

Esplanada dos Ministérios Bloco T, Ed. Sede - Bairro Zona Cívico Administrativa, Brasília/DF, CEP 70064-900
Telefone: 2025*3063/6942 e Fax: 2025*3000 - www.justica.gov.br

Ofício nº 164/2015/SIC SE/SE-MJ

Brasília, 16 de novembro de 2015.

Ao Senhor François

Assunto: Lei de Acesso à Informação – EXISTE ALGUM NORMATIVO QUE TRATE SOBRE OS EMAIL CORPORATIVOS OU CORREIOS ELETRÔNICOS PRODUZIDOS PELOS SERVIDORES NO DESEMPENHO DE SUAS ATIVIDADES? - **SIC/MJ Nº 08850.003463/2015-19.**

Prezado Senhor,

Reporto-me à Solicitação de Informação – SIC/MJ nº 08850.003463/2015-19, encaminhada por Vossa Senhoria em 26 de outubro de 2015 ao SIC CENTRAL MJ, para, nos termos da manifestação da Coordenação-Geral de Tecnologia da Informação – CGTI/MJ, encaminhar cópia do Despacho nº 1699/2015/DIARTI/CGTI/SPOA/SE (1367328), de 06 de novembro de 2015, bem como cópia da Portaria MJ nº 3.350, de 3 de dezembro de 2013, que institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça.

Atenciosamente,

EDUARDO SPANÓ JUNQUEIRA DE PAIVA
Ponto Focal da Secretaria Executiva

sei! assinatura eletrônica

Documento assinado eletronicamente por **EDUARDO SPANO JUNQUEIRA DE PAIVA**, **Ponto Focal do SIC SE**, em 16/11/2015, às 18:42, conforme o § 2º do art. 10 da Medida Provisória nº 2.200/01.

1367328 08850003463201519

MINISTÉRIO DA JUSTIÇA

Despacho nº 1699/2015/DIARTI/CGTI/SPOA/SE

Em, 06 de novembro de 2015.

Assunto: Resposta ao Despacho nº 1987/2015/CGTI/SPOA/SE
Destino: **CGTI - COORDENAÇÃO GERAL DE TECNOLOGIA DA INFORMAÇÃO**
Processo: **08850003463201519**

1. Em resposta ao Despacho nº 1987/2015/CGTI/SPOA/SE, referente à **SOLICITAÇÃO DE INFORMAÇÃO - SIC/MJ 08850.003463/2015-19 (SIC CENTRAL MJ),** informo o que se segue.

2. O Ministério da Justiça - MJ instituiu uma Política de Segurança da Informação e Comunicações - POSIC, publicada por meio da Portaria nº 3.530, de 03 de dezembro de 2013.

3. O art. 12 da POSIC menciona que 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.

4. Em conformidade ao inciso VII do art. 4º da POSIC, o órgão está em fase de elaboração de um normativo específico para fins de definição de regras claras e precisas de uso de seu e-mail institucional.

Atenciosamente,

Documento assinado eletronicamente por **LEO ROSSATO BISCAGLIA**, **Chefe da Divisão de Administração de Recursos de Tecnologia da Informação**, em 06/11/2015, às 19:04, conforme o § 2º do art. 10 da Medida Provisória nº 2.200/01.

Documento assinado eletronicamente por **MICHEL GOMES NOGUEIRA**, **Agente Administrativo**, em 09/11/2015, às 10:27, conforme o § 2º do art. 10 da Medida Provisória nº 2.200/01.

A autenticidade do documento pode ser conferida no site http://sei.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1367328** e o código CRC **DCBC8998**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça.

22 ISSN 1677-7042 Diário Oficial da União - Seção 1 Nº 235, quarta-feira, 4 de dezembro de 2013

Ministério da Justiça

GABINETE DO MINISTRO

PORTARIA Nº 3.525, DE 3 DE DEZEMBRO DE 2013

O MINISTRO DE ESTADO DA JUSTIÇA, com base no disposto na Lei nº 91, de 28 de agosto de 1935, regulamentada pelo Decreto nº 50.517, de 2 de maio de 1961, na Lei nº 9.784, de 29 de janeiro de 1999, usando da competência que lhe foi conferida pelo art. 1º, do Decreto nº 3.415, de 19 de abril de 2000, resolve:

Art. 1º Conhecer e dar provimento ao recurso apresentado pela entidade denominada INSTITUTOS PARAIBANOS DE EDUCAÇÃO - IPÊ - registrada no CNPJ sob o nº 08.679.5570001-02, pelos fundamentos presentes na Representação Administrativa nº 14751.000009/2011-01.

Art. 2º Revogar a Portaria Ministerial nº 1.097, de 25 de março de 2013, publicada no DOU de 26 de março de 2013, Seção 1, que cassou o título de Utilidade Pública Federal da entidade denominada INSTITUTOS PARAIBANOS DE EDUCAÇÃO - IPÊ.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.526, DE 3 DE DEZEMBRO DE 2013

O MINISTRO DE ESTADO DA JUSTIÇA, com base no disposto na Lei nº 91, de 28 de agosto de 1935, regulamentada pelo Decreto nº 50.517, de 2 de maio de 1961, e usando da competência que lhe foi delegada pelo art. 1º do Decreto nº 3.415, de 19 de abril de 2000, resolve:

Art. 1º Indeferir o pedido do Título de Utilidade Pública Federal da ASSOCIAÇÃO FILANTRÓPICA DOS TÉCNICOS ELETROTÉCNICA ELETRÔNICA E ELETRICISTA DO CEARÁ-AFTEC, com sede na cidade de Fortaleza, Estado do Ceará, registrada no CNPJ sob o nº 04.606.342/0001-00 (Processo MJ nº 08071.010175/2013-26).

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

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.527, DE 3 DE DEZEMBRO DE 2013

O MINISTRO DE ESTADO DA JUSTIÇA, em cumprimento à decisão liminar proferida pela 8ª Vara da Seção Judiciária do Distrito Federal, nos autos da Ação Ordinária nº 0027378-91.2013.4.01.3400, ajuizada por JOSÉ COSMO LOPES DE FREITAS, resolve:

I - SUSPENDER os efeitos da Portaria nº 884, de 22 de maio de 2012, publicada no DOU de 23 de maio de 2012, Seção 1, que anulou a Portaria Ministerial nº 1.920, de 25 de novembro de 2003, que declarou JOSÉ COSMO LOPES DE FREITAS anistiado político.

II - RESTABELECER os efeitos da Portaria Ministerial nº 1.920, de 25 de novembro de 2003, que declarou JOSÉ COSMO LOPES DE FREITAS anistiado político.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.528, DE 3 DE DEZEMBRO DE 2013

Dispõe sobre a prorrogação do emprego da Força Nacional de Segurança Pública em apoio ao Governo do Estado de Alagoas.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais e considerando o disposto na Lei nº 11.473, de 10 de maio de 2007, no Decreto nº 5.289, de 29 de novembro de 2004, na Portaria nº 3.383/MJ, de 24 de outubro de 2013 e no Acordo de Cooperação Federativa da Força Nacional de Segurança Pública nº 002/2011, publicado no D.O.U. nº 202, de 20 de outubro de 2011; e

Considerando a Operação Jaraguá, desenvolvida no Estado de Alagoas a fim de realizar ações de Segurança Pública em apoio aos órgãos integrantes do Sistema de Segurança Pública do supracitado Estado, conforme OG nº 200/13.01.1, de 11 de novembro de 2013, resolve

Art. 1º Autorizar a prorrogação do apoio da Força Nacional de Segurança Pública - FNSP, em caráter episódico e planejado, a partir da data de vencimento da Portaria nº 2.963, de 6 de setembro de 2013, e por mais 90 (noventa) dias, a contar da data de publicação desta Portaria, para exercer ações de Segurança Pública, atuando em conjunto com os órgãos integrantes do Sistema de Segurança Pública do Estado de Alagoas.

Art. 2º A operação terá o apoio logístico e a supervisão dos órgãos de segurança pública do ente federado solicitante, nos termos do convênio de cooperação firmado entre as partes, bem como a permissão de acesso aos sistemas de informações e ocorrências no âmbito da Segurança Pública durante a vigência desta Portaria.

Art. 3º O prazo do apoio prestado pela FNSP poderá ser prorrogado, se necessário, conforme o art. 4º, § 3º, inciso I, do Decreto nº 5.289, de 29 de novembro de 2004.

Art. 4º Esta Portaria entra em vigor a partir da data de sua publicação.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.529, DE 3 DE DEZEMBRO DE 2013

Redefine a denominação e as atribuições do Comitê Gestor de Tecnologia da Informação - CTI.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso das atribuições que lhe confere o art. 87, parágrafo único, incisos I e II, da Constituição, e tendo em vista o disposto no Decreto nº 7.579, de 11 de outubro de 2011, resolve:

Art. 1º O Comitê de Tecnologia da Informação passa a denominar-se Comitê Gestor de Tecnologia da Informação - CTI.

Art. 2º Compete ao CTI:

I - monitorar e avaliar a Política de Tecnologia da Informação do Ministério da Justiça - MJ por meio de um plano integrado de ações, considerando o Planejamento Estratégico do MJ e as políticas e orientações do Governo Federal;

II - sugerir a prioridade das demandas de Tecnologia da Informação - TI do MJ, inclusive de desenvolvimento de sistemas;

III - aprovar a proposta do Plano Diretor de Tecnologia da Informação - PDTI;

IV - aprovar a proposta do Plano de Investimento da área de TI;

V - zelar pela integração das iniciativas de Tecnologia da Informação e Comunicação;

VI - avaliar os sistemas de informação do MJ e aprovar suas atualizações, revisões e desativações;

VII - acompanhar o processo de contratações de soluções de TI com base no modelo de contratações de soluções de TI adotado pelo MJ, em consonância com o que regra a Secretaria de Logística e Tecnologia da Informação - SLTI do Ministério do Planejamento, Orçamento e Gestão - MP;

VIII - analisar os trabalhos e pareceres técnicos que forem encaminhados pelos grupos de trabalho, comissões técnicas e pela área de TI do MJ;

IX - estabelecer diretrizes básicas para a política de recursos humanos na área de TI do MJ;

X - participar de foro de debates com instituições que desenvolvam projetos de pesquisa ou estudos sobre informação e informática, bem como ser órgão difusor dessas participações junto ao MJ; e

XI - divulgar um cronograma de atividades do CTI para o exercício, sempre na primeira sessão ordinária.

Parágrafo único. Caberá ao CTI desenvolver ações estruturantes e de controle para a plena implantação do alinhamento estratégico e para o estabelecimento de metas anuais, em conformidade com o que determinar a Estratégia Geral de TI - EGTI vigente, ou, ainda, para o cumprimento dos compromissos periódicos acerca das demandas da área de TI.

Art. 3º O CTI será composto por um representante, titular e suplente, das seguintes unidades:

I - Gabinete do Ministro;
II - Secretaria Executiva;
III - Secretaria Executiva Adjunta;
IV - Subsecretaria de Planejamento, Orçamento e Administração;
V - Coordenação-Geral de Tecnologia da Informação;
VI - Comissão de Anistia;
VII - Consultoria Jurídica;
VIII - Departamento Penitenciário Nacional;
IX - Secretaria de Assuntos Legislativos;
X - Secretaria Nacional do Consumidor;
XI - Secretaria de Reforma do Judiciário;
XII - Secretaria Extraordinária de Segurança para Grandes Eventos;
XIII - Secretaria Nacional de Justiça;
XIV - Secretaria Nacional de Políticas sobre Drogas; e
XV - Secretaria Nacional de Segurança Pública.

§ 1º São considerados membros representantes titulares no CTI, preferencialmente, os Chefes de Gabinete das Secretarias Finalísticas e dos Departamentos constantes nos incisos I a XV do caput deste artigo e, na ausência de previsão regimental do cargo de chefe de gabinete, os servidores que exerçam a atribuição ou o encargo de chefe de gabinete, à exceção do Gabinete do Ministro que será representado pelo Coordenador-Geral do Gabinete.

§ 2º Os representantes titulares e seus respectivos suplentes serão indicados pelos dirigentes das unidades representadas no CTI e designados pela Secretaria Executiva.

§ 3º Nas ausências ou impedimentos, por motivo justificado, dos representantes titulares, serão convocados seus suplentes.

§ 4º A Secretaria Executiva indicará um representante, titular e suplente, responsável pela área de execução orçamentária e financeira, sem direito a voto.

§ 5º O CTI será coordenado pelo representante da Subsecretaria de Planejamento, Orçamento e Administração e em suas ausências ou impedimentos, pelo seu suplente.

§ 6º Poderão ser convidados a participar das reuniões do CTI, a juízo do seu Coordenador, para subsidiar suas deliberações, representantes de órgãos ou entidades públicas e privadas, bem como consultores técnicos, inclusive servidores públicos em exercício nos órgãos ou unidades integrantes da estrutura do MJ.

Art. 4º Compete ao Coordenador, ouvidos os demais membros do CTI:

I - criar grupos ou comissões para aprofundar debates e discussões sobre assuntos técnicos ou operacionais afetos às ações do CTI e indicar os coordenadores dentre os membros do CTI;

II - indicar representantes para participar de fóruns de debates com instituições que desenvolvam projetos de pesquisa ou estudos sobre informação e informática;

III - exercer outras atividades que lhe forem atribuídas em regimento interno; e

IV - submeter à ratificação do titular da Secretaria Executiva e do MJ o PDTI aprovado pelo CTI e o respectivo cronograma de execução, com a proposta das ações prioritárias.

Parágrafo único. Compete às autoridades constantes do inciso IV do caput deste artigo:

I - aprovar, alterar ou vetar o PDTI, total ou parcialmente;

II - aprovar, alterar ou vetar o Plano de Investimento de TI, total ou parcialmente; e

III - alterar, a qualquer tempo, a ordem de prioridade das ações de TI, inclusive de desenvolvimento de sistemas, em virtude de diretrizes estratégicas do MJ.

Art. 5º O apoio administrativo e os meios necessários à execução dos trabalhos do CTI serão prestados pela Coordenação-Geral de Tecnologia da Informação - CGTI, que funcionará como Secretaria Administrativa do CTI.

Art. 6º A participação no CTI é considerada como de relevante interesse público e não enseja nenhum tipo de remuneração.

Art. 7º O regimento interno será elaborado pelo CTI, no prazo de 120 (cento e vinte) dias, contados da data de publicação desta portaria e submetido à aprovação da Secretaria Executiva.

Art. 8º Fica revogada a Portaria GM/MJ nº 405, de 5 de março de 2012.

Art. 9º Esta Portaria entrará em vigor na data de sua publicação.

JOSÉ EDUARDO CARDOZO

PORTARIA Nº 3.530, DE 3 DE DEZEMBRO DE 2013

Institui a Política de Segurança da Informação e Comunicações do Ministério da Justiça, e dá outras providências.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso das atribuições que lhe conferem o art. 87, parágrafo único, inciso II, da Constituição, e o Decreto nº 6.061, de 15 de março de 2007, e tendo em vista o disposto no Decreto nº 3.505, de 13 de junho de 2000, e na Norma Complementar nº 3, de 30 de junho de 2009, do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República, resolve:

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicações do Ministério da Justiça - POSIC/MJ, na forma do Anexo a esta Portaria.

Art. 2º A POSIC/MJ aplica-se a todos os órgãos e entidades da estrutura organizacional do Ministério da Justiça.

Parágrafo único. Os órgãos e entidades de que trata o caput poderão elaborar políticas setoriais de segurança da informação e comunicações, desde que observados os princípios e as diretrizes gerais da POSIC/MJ.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

Art. 4º Fica revogada a Portaria nº 3.251, de 19 de dezembro de 2012, do Ministério da Justiça.

JOSÉ EDUARDO CARDOZO

ANEXO

CAPÍTULO I
DISPOSIÇÕES GERAIS

Art. 1º A Política de Segurança da Informação e Comunicações do Ministério da Justiça - POSIC/MJ objetiva dotar os órgãos e entidades da estrutura organizacional do Ministério de princípios, diretrizes, critérios e instrumentos aptos a assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações, protegendo-as contra ameaças e vulnerabilidades.

Art. 2º Para efeitos da POSIC/MJ, considera-se:

I - agente público: 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 no Ministério;

II - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado que possa resultar em dano para um sistema, órgão ou entidade da estrutura organizacional do Ministério;

III - ativos de informação: meios de armazenamento, transmissão e processamento de informação, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - 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;

V - confidencialidade: propriedade de que a informação não esteja disponível ou que não tenha sido revelada a pessoa física, sistema, órgão ou entidade não autorizados e não credenciados;

VI - continuidade de serviços: capacidade estratégica e tática de um órgão ou entidade da estrutura organizacional do Ministério de se planejar e responder a incidentes e interrupções de funcionamento, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

VII - disponibilidade: propriedade que assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou por determinado sistema, órgão ou entidade;

VIII - 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 e de implementar a segurança da informação e comunicações no Ministério;

IX - gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para um órgão ou entidade da estrutura organizacional do Ministério e os possíveis impactos no funcionamento de seus serviços e atividades, caso estas ameaças se concretizem;

X - 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, permitindo equilibrá-los com os custos operacionais e financeiros envolvidos;

XI - incidente de segurança: qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas de computação ou de redes de computadores;

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

XIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIV - Segurança da Informação e Comunicações - SIC: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XV - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; e

XVI - vulnerabilidade: conjunto de fatores internos ou causas potenciais de um incidente de segurança, que pode ser evitado por uma ação de SIC.

CAPÍTULO II

DO ESCOPO

Seção I

Dos Princípios

Art. 3º 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. 4º 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 pelos agentes públicos 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. 5º 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. 6º 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;

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. 7º 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. 8º O Comitê será composto por um representante, titular e suplente, de cada órgão e entidade a seguir indicados:

I - Gabinete do Ministro;
II - Comissão de Anistia;
III - Consultoria Jurídica;
IV - Secretaria Executiva;
V - Secretaria de Assuntos Legislativos;
VI - Secretaria Nacional de Justiça;
VII - Secretaria Nacional de Segurança Pública;
VIII - Secretaria de Reforma do Judiciário;
IX - Secretaria Nacional do Consumidor;
X - Secretaria Nacional de Políticas sobre Drogas;
XI - Secretaria Extraordinária de Segurança para Grandes Eventos;
XII - Departamento de Polícia Federal;
XIII - Departamento de Polícia Rodoviária Federal;
XIV - Departamento Penitenciário Nacional;
XV - Defensoria Pública da União;
XVI - Arquivo Nacional;
XVII - Conselho Administrativo de Defesa Econômica; e
XVIII - 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. 9º Fica criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, 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. 10. O acesso à Internet realizado por meio de ativos de tecnologia de informação e comunicações do Ministério deve ser autorizado, identificado e registrado.

Art. 11. Os registros de acessos aos ativos de informação do Ministério devem ser preservados em conformidade à legislação em vigor.

Art. 12. 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. 13. 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. 14. A POSIC/MJ e suas normas complementares deverão ser revisadas sempre que se fizer necessário, não excedendo o período máximo de dois anos.

PORTARIA Nº 3.537, DE 3 DE DEZEMBRO DE 2013

Dispõe sobre a atuação da Força Nacional de Segurança Pública em apoio ao estado da Bahia nas ações de segurança a serem desencadeadas por ocasião do Sorteio Final das Chaves para a Copa do Mundo FIFA Brasil 2014.

O MINISTRO DE ESTADO DA JUSTIÇA, no uso de suas atribuições legais e considerando o disposto na Lei nº 11.473, de 10 de maio de 2007, no Decreto nº 5.289, de 29 de novembro de 2004, na Portaria nº 3.383, de 24 de outubro de 2013 e no Acordo de Cooperação Federativa da Força Nacional de Segurança Pública nº 18/2012, celebrado entre a União e o Estado da Bahia, publicado no Diário Oficial da União nº 227, de 26 de novembro de 2012; e

Considerando a manifestação expressa do Governador do Estado da Bahia, quanto à necessidade do emprego da Força Nacional de Segurança Pública (FNSP), com o propósito de atuar nas ações de segurança a serem desencadeadas por ocasião do Sorteio Final das Chaves para a Copa do Mundo FIFA Brasil 2014, no município de Mata de São João, Costa de Sauípe/BA, conforme solicitação contida no Ofício nº 117/2013/GG, de 26 de novembro de 2013, resolve:

Art. 1º Autorizar o emprego da Força Nacional de Segurança Pública (FNSP), em caráter episódico e planejado, por 07 (sete) dias, a contar da data de publicação desta portaria, para atuar em ações de segurança a serem desencadeadas por ocasião do Sorteio Final das Chaves para a Copa do Mundo FIFA Brasil 2014, através de contingência para Controle de Tumultos e Distúrbios Civis, escolta e segurança aproximada dos Membros do Comitê Executivo da FIFA, a fim de preservar a ordem pública e garantir a integridade física dos envolvidos.

Art. 2º A operação terá o apoio logístico e a supervisão dos órgãos de segurança pública do Ente Federado solicitante, nos termos do convênio de cooperação firmado entre as partes, bem como permissão de acesso aos sistemas de informações e ocorrências no âmbito da Segurança Pública, durante a vigência da portaria autorizativa.

Art. 3° O número de policiais a ser disponibilizado pelo Ministério da Justiça obedecerá ao planejamento definido pelos entes envolvidos na operação.

Art. 4º O prazo do apoio prestado pela FNSP poderá ser prorrogado, se necessário, conforme o art. 4º, § 3º, inciso I, do Decreto nº 5.289, de 2004.

Art. 5º Esta Portaria entra em vigor na data de sua publicação.

JOSÉ EDUARDO CARDOZO

Anexo B

Documentos enviados como anexo pelo Ministério do Desenvolvimento, Indústria e Comércio

Parte da Portaria nº 12, de 24 de maio de 2006

CAPÍTULO II
CORREIO ELETRÔNICO

Art. 9º. O serviço de correio eletrônico mantido pelo Ministério, transitará por caixas postais e será colocado à disposição de seus servidores, empregados prestadores de serviço e estagiários. Este serviço representa ferramenta de trabalho de sua propriedade e, portanto, seu uso deverá estar afeto ao interesse do serviço, restringindo-se o envio de mensagens particulares ao mínimo indispensável.

Art. 10. Empregados prestadores de serviço, estagiários e bolsistas poderão, a critério do responsável pela área onde venham atuar, no interesse do serviço e durante o período de atuação no âmbito do Ministério, ter acesso ao correio eletrônico, observadas as normas desta portaria.

Art. 11. O serviço de correio eletrônico permite a transferência de documentos eletrônicos, através de uma infra-estrutura padronizada de serviço de tratamento de mensagens e documentos eletrônicos, conforme critérios abaixo:

I - o acesso ao software de correio eletrônico será realizado com permissão incluída no perfil do usuário cadastrado na rede;
II - a caixa postal (**mailbox**), incluindo-se mensagens recebidas (inbox), enviadas (sent itens), excluídas (deleted itens) e armazenadas, terá seu tamanho definido de acordo com o perfil do usuário, conforme indicação a seguir:
a) Cargo de Ministro de Estado e de Natureza Especial - **NES** = sem limite
b) Caixas Postais Institucionais = 100 Mb;
c) DAS nível 3 a 6 = 50 Mb;
d) Demais = 30 Mb.

III – os arquivos eventualmente anexados às mensagens recebidas e expedidas deverão estar condicionados à disponibilidade de espaço na caixa postal.
IV - quando ultrapassados os limites de Mb estabelecidos, ocorrerá o bloqueio automático deste serviço até que o usuário exclua as mensagens ou as transfira para pastas particulares. Essa ocorrência será precedida de mensagens automáticas, alertando o usuário sobre o esgotamento da capacidade de sua caixa postal;
V – ocorrendo o bloqueio total de uma caixa postal e não tendo sido tomada providência por parte de seu titular, no sentido de solucionar o problema, a CGMI emitirá memorando de alerta, orientando sobre os procedimentos a serem adotados. Caso persista o impasse, sem justificativas, a CGMI poderá eliminar todo o conteúdo da caixa postal, sem geração de backup.
VI – casos excepcionais, onde fique demonstrada a necessidade de uso de maiores espaços na caixa postal, deverão ser submetidos à CGMI, que poderá atender à demanda, havendo disponibilidade nos servidores e sem prejuízo aos demais usuários.

Art. 12. Todos os usuários que possuem um **login** de acesso à rede, recebem conjuntamente, uma caixa de correio eletrônico (**e-mail**) destinada às comunicações internas e externas, através da INTERNET. O endereço de e-mail é formado pelo nome.sobrenome, acrescido do domínio do MDIC na INTERNET, o que resulta em: nome.sobrenome@desenvolvimento.gov.br.

Parágrafo único. Os casos excepcionais deverão ser submetidos à aprovação do Coordenador-Geral de Modernização e Informática – CGMI, que poderá autorizar a utilização de outro endereço eletrônico.

Art. 13. As caixas postais de destino e origem de correio eletrônico estarão divididas em grupos de caixas postais individuais e caixas postais institucionais:

I - As caixas postais individuais destinam-se ao recebimento/emissão de mensagens, cujo cunho seja eminentemente pessoal.
II - As caixas postais institucionais destinam-se ao recebimento/emissão de mensagens estritamente vinculadas aos serviços, produtos e atividades do Ministério e serão acessadas apenas por funcionários expressamente autorizados pelas autoridades de cada unidade e cadastrados no servidor do Ministério. Os nomes destas caixas postais serão formados pela sigla de identificação da unidade, conforme o regimento interno, seguida do domínio do MDIC.

Art. 14. Atos administrativos internos do Ministério, enviados ou recebidos pelo correio eletrônico, envolvendo em sua origem e destino caixas postais institucionais, serão considerados documentos oficiais, desde que não envolvam solicitações ou autorizações para realização de dispêndios.

Art. 15. O correio eletrônico poderá ser acessado internamente, através da utilização de programas de correio corporativo e externamente através do recurso **Web Access**, que permite o acesso à caixa postal a partir de qualquer computador conectado à INTERNET, utilizando um **browser** comum (**INTERNET EXPLORER, Fire Fox, Opera**, etc.).

Art. 16. As mensagens recebidas pelos usuários e mantidas em sua caixa postal serão preservadas pelo sistema de **backup** diário, efetuado ao final do expediente, garantindo a recuperação das mensagens no caso de falhas, de rastreamento contra **vírus** anexados às mensagens enviadas ou recebidas ou de segurança contra a violação de sua privacidade. A garantia de privacidade está diretamente relacionada à manutenção do sigilo da senha pelo usuário.

Art. 17. Poderão ser criados grupos de discussão, destinados exclusivamente ao trato de assuntos inerentes ao interesse do Ministério, ficando o gerenciamento sob a responsabilidade do órgão que solicitou a formação dos grupos.

Art. 18. Fica terminantemente proibido o uso das caixas postais para listas de distribuição, veiculação de mensagens de grupos de afinidades e mensagens circulares não vinculadas ao interesse do Ministério, e o uso das caixas postais institucionais para trânsito de mensagens de caráter pessoal.

Parágrafo único. A utilização indevida das caixas postais acarretará, na primeira ocorrência, a edição de advertência formal ao titular da caixa de origem. Em caso de reincidência, haverá a suspensão de uso, somente liberado após solicitação do superior imediato do titular da caixa de origem. Em caso de nova utilização indevida, a suspensão será pelo prazo de 90 (noventa) dias, independentemente de comunicação ao superior imediato.

Art. 19. A CGMI fica autorizada a promover limitações de acesso à rede mundial de computadores, com o objetivo de eliminar, antes de sua chegada aos destinatários, os e-mail que contenham arquivos incompatíveis com os serviços realizados no âmbito do Ministério, respeitando-se o sigilo das comunicações.

Art. 20. Deverão ser comunicadas tempestivamente à CGMI:

a) todos os afastamentos de servidores, superiores a três meses, bem como a desvinculação definitiva de servidores, estagiários e bolsistas, pela Coordenação-Geral de Recursos Humanos - CGRH; e
b) o desligamento de empregados prestadores de serviço, pelos gestores de contratos.

Parágrafo único. No caso de afastamento definitivo a CGMI providenciará a exclusão da caixa postal.

Anexo C
Documentos enviados como anexo pelo Ministério da Defesa

GABINETE DO MINISTRO
PORTARIA NORMATIVA Nº 1.530/MD, DE 14 DE MAIO DE 2013

Aprova a Política de Segurança da Informação e Comunicações da Administração Central do Ministério da Defesa e dá outras providências.

O MINISTRO DE ESTADO DA DEFESA, no uso das atribuições que lhe são conferidas pelos incisos I e II do parágrafo único do art. 87 da Constituição, tendo em vista o disposto no Decreto nº 3.505, de 13 de junho de 2000; nos incisos XV e XVII do art. 27; nos incisos II, III, IV e V do art. 31 do Anexo I do Decreto nº 7.974, de 1º de abril de 2013, e em conformidade com o art. 98 da Lei nº 12.702, de 7 de agosto de 2012, resolve:

Art. 1º Aprovar, nos termos do Anexo a esta Portaria Normativa, a Política de Segurança da Informação e Comunicações (PoSIC), com a finalidade de fornecer diretrizes, critérios e suporte administrativo para a implementação da Segurança da Informação e Comunicações (SIC) no âmbito da Administração Central do Ministério da Defesa (ACMD).

Parágrafo único. A PoSIC se aplica às atividades dos usuá-rios da ACMD e os obriga ao cumprimento de suas diretrizes para manuseio, tratamento, controle, proteção das informações e conhecimentos produzidos, armazenados ou transmitidos pelos sistemas de informação ou por meio de outros recursos.

Art. 2º O Centro Gestor e Operacional do Sistema de Proteção da Amazônia (Censipam), o Hospital das Forças Armadas (HFA) e o Centro de Catalogação das Forças Armadas (Cecafa), devido às suas especificidades, serão regidos por Política de Segurança de Informação e Comunicações própria, alinhada, no que couber, à PoSIC anexa a esta Portaria Normativa, a qual deve ser submetida, no prazo de noventa dias, à avaliação e à aprovação do Comitê de Segurança da Informação e Comunicações (CSIC).

Art. 3º A íntegra da PoSIC da ACMD será disponibilizada no endereço eletrônico www.defesa.gov.br, no Portal do Ministério da Defesa (MD) e também em sua Intranet.

Art. 4º Esta Portaria Normativa entra em vigor na data de sua publicação.

CELSO AMORIM

ANEXO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES
DA ADMINISTRAÇÃO CENTRAL DO MINISTÉRIO DA DEFESA

1. ESCOPO

1.1. A Política de Segurança da Informação e Comunicações (PoSIC) tem por objetivo instituir e implementar diretrizes estratégicas, responsabilidades e competências que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade (DICA)das informações no âmbito da Administração Central do Ministério da Defesa (ACMD).

1.2. A PoSIC trata do uso e do compartilhamento de dados, informações e documentos no âmbito da ACMD, em todo o seu ciclo de vida (criação, manuseio, divulgação, armazenamento, transporte e descarte), visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

2. CONCEITOS E DEFINIÇÕES

2.1. Para os efeitos desta Política entende-se por:

a) Assinatura digital: conjunto de dados criptografados, associados a determinado documento/arquivo que foi assinado, destinado a garantir a autenticidade e a integridade das informações constantes do documento, sua autoria e eventuais modificações;

b) Ativo de informação: patrimônio composto por dados, informações e conhecimentos obtidos, gerados e manipulados durante a execução dos sistemas e processos de trabalho;

c) Comitê de Segurança da Informação e Comunicações: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da ACMD;

d) Computação em nuvem: modelo computacional que permite acesso, por demanda e independente da localização, a 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;

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

f) Custodiante da informação: usuário que atua em uma ou mais fases do tratamento da informação, ou seja: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, incluindo a sigilosa;

g) Dispositivos móveis: equipamentos portáteis, dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, dentre eles: notebooks, netbooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória;

h) Equipe de tratamento e resposta a incidentes em redes computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;

i) Gestão de continuidade: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece estrutura para que se desenvolva uma resiliência organizacional capaz de responder efetivamente e salvaguardar os interesses das partes envolvidas, a reputação e a marca da organização, assim como seus processos e de valor agregado. É o resultado da fusão dos Planos de Contingência e dos Planos de Recuperação de Desastres, que objetiva garantir a recuperação de um ambiente de produção, independentemente de eventos que suspendam suas operações e de danos nos componentes (processos, pessoas softwares, hardware, infraestrutura etc.) por ele utilizados;

j) Gestão de 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 (TIC);

k) Gestão de Riscos em Segurança da Informação e 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;

l) Gestor de Segurança da Informação e Comunicações: responsável pelas ações de segurança da informação e comunicações no âmbito da ACMD;

m) Infraestrutura crítica de TIC: conjunto dos ativos de tecnologia da informação que afetam diretamente a consecução e a continuidade da informação por meios tecnológicos;

n) Inventário e Mapeamento de Ativos de Informação: processo interativo e evolutivo, composto por três etapas:

a) identificação e classificação de ativos de informação;

b) identificação de potenciais ameaças e vulnerabilidades;

c) avaliação de riscos;

o) Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;

p) Recurso criptográfico: sistemas, programas, processos e equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

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

r) Termo de Compromisso Individual (TCI): documento formal, a ser assinado pelos usuários da ACMD, por meio do qual é estabelecido vínculo de comprometimento pessoal com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

s) Tratamento da informação: recepção, produção, reprodu-ção, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas;

t) Usuários: servidores, militares, terceirizados, colaboradores, consultores, auditores, estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de informação da ACMD, formalizada por meio da assinatura do TCI.

3. REFERÊNCIAS

3.1.A PoSIC da ACMD foi elaborada com base nas seguintes referências legais e normativas:

- Lei nº 8.112, de 11 de dezembro de 1990;
- Lei nº 9.983, de 14 de julho de 2000;
- Lei nº 12.527, de 18 de novembro de 2011;
- Decreto nº 3.505, de 13 de junho de 2000;
- Decreto nº 4.553, de 27 de dezembro de 2002;
- Decreto nº 5.482, de 30 de junho de 2005;
- Decreto nº 7.974, de 1º de abril de 2013;
- Instrução Normativa GSI nº 1, de 13 de junho de 2008, e respectivas normas complementares;
- Portaria Normativa nº 142/MD, de 25 de janeiro de 2008;
- Portaria Normativa nº 1.704/MD, de 27 de junho de 2012;
- Norma ABNT NBR/ISO/IEC 27001/2006;
- Norma ABNT NBR/ISO/IEC 27002/2007;
- Decreto nº 7.724, de 16 de maio de 2012;
- Decreto nº 7.845, de 14 de novembro de 2012.

4. PRINCÍPIOS

4.1.A PoSIC da ACMD orienta-se pelos seguintes princípios:

a) Disponibilidade: garante que a informação estará acessível e utilizável por pessoa física, sistema, órgão ou entidade, quando requisitada;

b) Integridade: garante que a informação não será modificada, gravada ou excluída sem autorização ou acidentalmente;

c) Confidencialidade: garante que a informação será acessada apenas por pessoa física, sistema, órgão ou entidade autorizada e credenciada;

d) Autenticidade: garante a identificação de pessoa física, sistema, órgão ou entidade que produziu, expediu, modificou ou excluiu a informação.

4.2.As ações de segurança da informação e comunicações da ACMD são norteadas pelos seguintes princípios:

a) Criticidade: define a importância da informação para a continuidade do negócio da organização;

b) Celeridade: garante respostas rápidas a incidentes e falhas de segurança;

c) Clareza: as regras e a documentação sobre segurança da informação e comunicações devem ser elaboradas de forma clara, precisa, concisa e de fácil entendimento;

d) Ética: preserva o direito do servidor, militar, colaborador, estagiário e prestador de serviços, sem que ocorra o comprometimento da segurança da informação e comunicações;

e) Legalidade: devem ser levadas em consideração as leis, as normas e as políticas organizacionais administrativas, técnicas e operacionais vigentes;

f) Responsabilidade: os usuários são responsáveis pelo cumprimento da Política de Segurança da Informação e Comunicações e devem respeitar a legislação e normas pertinentes à segurança da informação e comunicações.

4.3.São observados, ainda, sem prejuízo dos demais, os princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a APF.

5. DIRETRIZES GERAIS

5.1.Pressupostos básicos

5.1.1. O sucesso das ações nos assuntos de segurança da informação e comunicações está diretamente associado à capacitação científico-tecnológica dos recursos humanos envolvidos, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

5.1.2. A informação é um recurso vital para o adequado funcionamento de toda e qualquer organização, devendo ser tratada como patrimônio a ser protegido e preservado.

5.2.Para cada uma das diretrizes constantes das Seções deste Capítulo devem ser elaboradas normas técnicas específicas, manuais e procedimentos.

5.3.Tratamento da Informação

5.3.1. Toda informação criada, adquirida ou custodiada pelo usuário, no exercício de suas atividades, é considerada bem e propriedade do MD e deve ser protegida segundo as diretrizes descritas nesta PoSIC e demais regulamentações em vigor, com o objetivo de minimizar riscos às atividades e serviços do Órgão e preservar sua imagem.

5.3.2. É expressamente proibido o acesso, a guarda ou o encaminhamento de material discriminatório, malicioso, não ético, obsceno ou ilegal por intermédio de quaisquer meios e recursos de tecnologia da informação disponibilizados pelo MD.

5.3.3. Os ativos de informação devem ser protegidos de forma preventiva, com o objetivo de minimizar riscos às atividades e aos objetivos de negócio do MD.

5.3.4. As informações criadas, armazenadas, manuseadas, transportadas ou descartadas devem ser classificadas segundo o grau de sigilo, criticidade e outros, conforme normas internas e legislação específica em vigor.

5.3.5. Todo usuário deve respeitar a classificação atribuída a uma informação e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

5.3.6. As informações produzidas ou custodiadas pelo MD devem ser descartadas conforme o seu nível de classificação.

5.3.7. Deve ser disponibilizado Sistema de Gestão Eletrônica de Documentos com mecanismos de assinatura digital aderente à legislação em vigor, com a finalidade de mitigar riscos associados à informação impressa.

5.3.8. A manipulação de informações classificadas em qualquer grau de sigilo deve seguir as normas internas e a legislação em vigor.

5.4.Tratamento de Incidentes de Rede

5.4.1 A área de Tecnologia da Informação (TI) do MD manterá Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores.

5.5.Gestão de Risco

5.5.1. Os riscos devem ser continuamente monitorados e tratados, de acordo com as vulnerabilidades associadas aos ativos de informação e aos níveis de risco, conforme procedimentos definidos em norma específica sobre gestão de riscos em segurança da informação e comunicações.

5.5.2. Os usuários são responsáveis por adotar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos seus ativos de informação no âmbito da ACMD.

5.5.3. O processo de inventário e mapeamento de ativos de informação deve ser aplicado tanto na gestão de riscos quanto na gestão de continuidade, conforme procedimentos definidos em norma específica sobre o tema.

5.6.Gestão de Continuidade

5.6.1. O MD deve manter processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.

5.6.2. As informações de propriedade ou custodiadas pelo MD, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança, de forma a garantir a continuidade das atividades do Órgão.

5.6.3.As informações armazenadas em outros meios devem
possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

5.7.Auditoria e Conformidade

5.7.1. q O MD deve criar e manter registros e procedimentos, como trilhas de auditoria, que possibilitem o rastreamento, o
acompanhamento, o controle e a verificação de acessos aos sistemas
corporativos e rede interna do MD.

5.7.2. Deve ser realizada, com periodicidade mínima anual,
verificação de conformidade das práticas de SIC do MD com esta
PoSIC e procedimentos complementares, bem como com a legislação
específica em vigor.

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

5.7.4.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.

5.7.5.Os resultados de cada ação de verificação de conformidade serão documentados em Relatório de Avaliação de Conformidade.

5.8.Controle de Acesso

5.8.1.O controle de acesso aos sistemas corporativos, o credenciamento de acesso de usuários aos ativos de informação e o acesso às informações em áreas e instalações consideradas críticas devem ser implantados nos níveis físico e lógico definidos em norma específica, em conformidade com as diretrizes desta PoSIC.

5.9.Uso de E-mail (Correio Eletrônico)

5.9.1.O uso de e-mail no âmbito da ACMD deve ser definido em norma específica, com controle do uso e cancelamento de acesso ao correio eletrônico.

5.10.Acesso à Internet

5.10.1.O acesso à rede mundial de computadores (Internet), no âmbito da ACMD, será regido por norma interna, em conformidade com as diretrizes desta PoSIC, orientações governamentais e legislações específicas em vigor.

5.11.Inventário e Mapeamento de Ativos de Informação

5.11.1.O processo de Inventário e Mapeamento de Ativos de Informação deve produzir subsídios tanto para a Gestão de Segurança da Informação e Comunicações, a Gestão de Riscos de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios, nos aspectos relacionados à segurança da informação e

comunicações, quanto para os procedimentos de avaliação da conformidade, de melhorias contínuas, auditoria e, principalmente, de estruturação e geração de base de dados sobre os ativos de informação.

5.11.2. O processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado, para manter a Base de Dados de Ativos de Informação atualizada e, consequentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

5.12.Dispositivos Móveis

5.12.1.O uso de dispositivos móveis para acesso aos recursos computacionais no âmbito da ACMD deve ser controlado, com a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, de acordo com procedimentos definidos em norma específica e em conformidade com as diretrizes desta PoSIC.

5.13.Computação em Nuvem

5.13.1. As ações de segurança da informação e comunicações para a implementação ou a contratação, no âmbito da ACMD, de tecnologias de computação em nuvem devem estar em conformidade com as orientações definidas em norma e legislações específicas em vigor.

5.14.Criptografia

5.14.1.A cifração e a decifração de informações classificadas em qualquer grau de sigilo devem utilizar recurso criptográfico baseado em algoritmo de Estado, conforme procedimentos definidos em norma e legislações específicas em vigor.

5.15.Redes Sociais

5.15.1.O uso institucional das redes sociais deve ser norteado por diretrizes, critérios, limitações e responsabilidades estabelecidas, visando ao uso seguro das redes sociais, conforme procedimentos definidos em norma específica e legislações específicas em vigor.

5.16.Contratação de Serviços

5.16.1. Nos editais de licitação e nos contratos de empresas prestadoras de serviços com a ACMD deverá constar cláusula específica sobre a obrigatoriedade de atendimento às normas desta PoSIC, bem como ser exigida da empresa contratada e do prestador a assinatura do Termo de Compromisso Individual e do Termo de Confidencialidade.

5.16.2. A empresa contratada também deverá demonstrar que possui mecanismos formais, no mínimo iguais aos adotados nesta PoSIC, que assegurem a confidencialidade e a segurança das informações.

5.16.3. Não deve ser adotada como prática a contratação de serviços terceirizados para atuação na Segurança da Informação e Comunicações, bem como na Infraestrutura Crítica de Tecnologia da Informação e Comunicações.

6. PENALIDADES

6.1.O usuário responderá pelo prejuízo que vier a ocasionar ao MD em decorrência do descumprimento de uma ou mais regras previstas nesta PoSIC.

6.2.A desobediência às regras estabelecidas implicará ao infrator as penalidades previstas em lei, nos âmbitos administrativo, civil, penal e militar.

7. COMPETÊNCIAS E RESPONSABILIDADES

7.1.Gestor de Segurança da Informação e Comunicações:

7.1.1. Planejar e coordenar a execução das ações de SIC;

7.1.2. Definir estratégias para a implementação desta PoSIC e normas complementares;

7.1.3. Supervisionar e analisar a efetividade dos processos, procedimentos, sistemas e dispositivos de SIC;

7.1.4. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e adotar as medidas administrativas necessárias à aplicação de ações corretivas;

7.1.5. Encaminhar os fatos apurados, decorrentes de quebras de segurança, para a aplicação das penalidades previstas;

7.1.6. Gerenciar a análise de risco;

7.1.7. Verificar se os procedimentos de Segurança da Informação e Comunicações (SIC) estão sendo aplicados de forma a atender à conformidade com legislações vigentes a respeito do assunto e normativos internos específicos;

7.1.8. Providenciar a divulgação interna e permanente desta PoSIC.

7.2.Comitê de Segurança da Informação e Comunicações:

7.2.1. Atualizar a Política de Segurança da Informação e Comunicações;

7.2.2. Propor grupos de trabalho para tratar de temas e sugerir soluções específicas sobre a segurança da informação e comunicações;

7.2.3. Propor, analisar e aprovar normas relativas à segurança da informação e comunicações, em conformidade com as legislações vigentes sobre o tema;

7.2.4. Propor um programa de Gestão de Continuidade de Negócios, com vistas a minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do MD, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação.

7.3.Setor de Tecnologia da Informação:

7.3.1. Planejar, coordenar, supervisionar, executar e controlar a execução das atividades de TIC relacionadas com as diretrizes desta PoSIC;

7.3.2. Elaborar, implementar e atualizar normas internas específicas em conformidade com esta PoSIC e demais diretrizes do Governo;

7.3.3. Criar e manter a ETIR, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em rede de computadores;

7.3.4. Manter registros e procedimentos como trilhas de auditoria e outros que assegurem o rastreamento, o acompanhamento, o controle e a verificação de acesso a todos os sistemas corporativos e das redes computacionais do MD;

7.3.5. Criar e manter a Assessoria de Segurança da Informação e Comunicações (ASSIC), com a responsabilidade de apoiar o Gestor de Segurança da Informação e Comunicações no cumprimento de suas atribuições;

7.4.Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais:

7.4.1.Facilitar e coordenar as atividades de tratamento e resposta a incidentes de segurança;

7.4.2.Promover a recuperação de sistemas;

7.4.3.Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de rede por meio de verificações de conformidade;

7.4.4.Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

7.4.5.Analisar ataques e intrusões na rede do MD;

7.4.6.Executar as ações necessárias para tratar quebras de segurança;

7.4.7.Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

7.4.8.Cooperar com outras equipes de Tratamento e Resposta a Incidentes.

7.5.Setor de Recursos Humanos:

7.5.1. Comunicar ao Gestor de SIC, por meio de memorando, a ausência ou o desligamento de pessoal do MD;

7.5.2. Definir, nas descrições de cargos e funções, as responsabilidades pela manutenção das ações de SIC, bem como colher a assinatura do Termo de Compromisso Individual que envolva o manuseio dos ativos de informação;

7.5.3.Promover a ambientação de todo o pessoal, civil e militar, nomeado e/ou designado para a ACMD, por meio de treinamento e capacitação, com vistas a permitir acesso aos sistemas corporativos e às informações nos níveis físico e lógico, definidos em norma específica, em conformidade com as diretrizes desta PoSIC.

7.6.Usuário:

7.6.1.Acessar a rede de dados do MD somente após tomar ciência das normas de SIC e assinar o TCI;

7.6.2.Tratar a informação digital como patrimônio do MD e como recurso que deva ter seu sigilo preservado;

7.6.3.Utilizar as informações digitais disponibilizadas e os sistemas e produtos computacionais de propriedade ou direito de uso da MD exclusivamente para o interesse do serviço;

7.6.4.Preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

7.6.5.Não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a sua Credencial de Segurança (CredSeg) ou cujo teor não tenha autorização ou necessidade de conhecer;

7.6.6.Não se fazer passar por outro usuário usando a identificação de acesso (login) e senha de terceiros;

7.6.7.No caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o sigilo das informações e documentos sigilosos a que teve acesso;

7.6.8.Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas autenticações de acesso (senhas) utilizadas no ambiente computacional do MD por terceiros;

7.6.9.Responder, perante o MD, por acessos, tentativas de acesso ou uso indevido da informação digital, realizados com a sua identificação ou autenticação;

7.6.10. Não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

7.6.11. Não transferir qualquer tipo de arquivo que pertença ao MD para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

7.6.12. Estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional do MD;

7.6.13. Estar ciente de que toda informação digital armazenada, processada e transmitida no ambiente computacional do MD pode ser auditada;

7.6.14. Estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e que qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da ACMD deve obedecer a esse preceito;

7.6.15. Ao assinar o TCI, o usuário declara, formalmente, ter pleno conhecimento e aceitar expressamente, sem reservas, os termos desta PoSIC.

7.7.Custodiante da Informação:

7.7.1. Cumprir e zelar pela observância integral das diretrizes desta PoSIC e demais normas e procedimentos decorrentes;

7.7.2. Zelar pela disponibilidade, integridade, confidencialidade e autenticidade das informações e recursos em qualquer suporte sob sua custódia, conforme condições estabelecidas nesta PoSIC e demais normas e procedimentos decorrentes, mediante assinatura do TCI;

7.7.3. Participar de capacitação e treinamento em segurança da informação e comunicações, quando convocado;

7.7.4. Utilizar os recursos que lhe foram concedidos somente para o fim a que se destinam;

7.7.5. Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada;

7.7.6. Preservar a classificação do grau de sigilo a documentos, dados e informações dos quais tiver conhecimento em decorrência do exercício de suas funções;

7.7.7.Comunicar prontamente ao seu Chefe imediato e ao Gestor de Segurança da Informação e Comunicações qualquer incidente de que tenha conhecimento ou situações que comprometam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e recursos em qualquer suporte sob sua custódia.

8.DIVULGAÇÃO

8.1. A PoSIC e suas atualizações, após publicação, deverão ser divulgadas amplamente aos usuários da ACMD e disponibilizadas no Portal do MD e também em sua Intranet.

9. ATUALIZAÇÃO

9.1.A atualização desta PoSIC e instrumentos normativos adicionais obedecerão aos seguintes critérios:

9.1.1.Política - Nível de Aprovação: Ministro de Estado da Defesa. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de três anos;

9.1.2.Normas - Nível de Aprovação: Comitê de Segurança da Informação e Comunicações. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de dois anos;

9.1.3.Procedimentos - Nível de Aprovação: Responsável pela área envolvida. Periodicidade de atualização: sempre que se fizer necessário, não excedendo o período máximo de um ano.

10.ANEXOS

10.1.Termo de Compromisso Individual.

10.2.Termo de Confidencialidade.

ANEXO I

MINISTÉRIO DA DEFESA
SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL DEPARTAMENTO DE TECNOLOGIA DA INFORMA-ÇÃO E COMUNICAÇÕES
TERMO DE COMPROMISSO INDIVIDUAL

Pelo presente instrumento, eu, _____, CPF no _____, Carteira de Identidade no _____, expedida pelo _____ em _____, lotado (a) no (a) _____, neste Ministério, na qualidade de USUÁRIO (A) da rede de computadores ou CUSTODIANTE de informações da Administração Central do Ministério da Defesa, DECLARO TER CONHECIMENTO da Política de Segurança da Informação e Comunicações (PoSIC) da ACMD, segundo a qual, sem restar qualquer dúvida de minha parte, devo:

a) tratar a informação como patrimônio do MD;

b) utilizar as informações e os recursos, em qualquer suporte sob minha custódia, exclusivamente no interesse do serviço do MD;

c) manter a confidencialidade das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas e/ou que não tenham necessidade de conhecê-las;

d) utilizar as credenciais de acesso (login e senha) e os recursos computacionais, em conformidade com a PoSIC da ACMD e procedimentos estabelecidos em normas específicas do Órgão;

e) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, observar a confidencialidade das informações sigilosas acessadas;

f) responder perante o MD pelo uso indevido das minhas credenciais de acesso, no âmbito administrativo e, se for o caso, perante a Justiça, no âmbito penal e civil.

Estou ciente de meu compromisso individual no Ministério da Defesa e assumo a responsabilidade pelas consequências decorrentes da não observância do disposto no presente Termo e na legislação vigente.

Brasília - DF, de de .

_____

Assinatura
(Usuário)

_____

Assinatura
(Representante da Assessoria de Segurança da Informação e Comunicações)

ANEXO II

MINISTÉRIO DA DEFESA
SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÕES
TERMO DE CONFIDENCIALIDADE

A _____, inscrita no CNPJ sob o nº _____, sediada _____, por intermédio de seu representante legal, Sr(a). _____, portador(a) da Cédula de Identidade nº _____, expedida pela(o) _____ e CPF nº _____, DECLARA que, para fins da execução do contrato no _____, comprometemo-nos a manter em sigilo, ou seja, não revelar ou divulgar as informações confidenciais ou de caráter não público recebidas durante e após a prestação dos serviços nas instalações do Ministério da Defesa, tais como: informações técnicas, operacionais, administrativas, econômicas, financeiras e quaisquer outras informações, escritas ou verbais, fornecidas ou que venham a ser de nosso conhecimento, sobre os serviços licitados, ou que a eles se referem.

A violação dos termos deste instrumento resultará na aplicação das penalidades cabíveis ao infrator, cíveis e criminais, nos termos da lei, obrigando-lhe, ainda, a isentar e/ou indenizar o Ministério da Defesa de todo e qualquer dano, perda, prejuízo ou responsabilidade, em virtude de demandas, ações, danos, perdas, custas e despesas que porventura venha a sofrer como resultado da violação do disposto neste instrumento.

_____

Local e Data

_____

Nome, Cargo e Assinatura do Representante da Licitante

Este texto não substitui o publicado do DOU de 16.05.2013, N°93, Seção 1; Página 33

(Boletim nº 06/2006):
INSTRUÇÃO NORMATIVA Nº 003/SEORI/MD, DE 22 DE FEVEREIRO DE 2006.

Define os critérios para utilização do serviço de correio eletrônico corporativo da administração central do Ministério da Defesa, visando a disciplinar a troca de mensagens eletrônicas, nos âmbitos interno e externo, e dá outras providências.

O SECRETÁRIO DE ORGANIZAÇÃO INSTITUCIONAL, no uso das atribuições que lhe são conferidas pelo inciso XV do art. 20 do Anexo I do Decreto nº 5.201, de 2 de setembro de 2004, resolve:

Art. 1º Definir os critérios para utilização do serviço de correio eletrônico corporativo da administração central do Ministério da Defesa, visando a disciplinar a troca, interna e externa, de mensagens eletrônicas.

Art. 2º Entende-se por serviço de correio eletrônico a ferramenta que possibilita a transferência de todo e qualquer documento eletrônico com conteúdo, equivalente ou não à obra literária, para fins de comunicação no âmbito da administração central do Ministério da Defesa.

Art. 3º O Ministério da Defesa, por meio do Departamento de Administração Interna – DEADI, disponibilizará, como ferramenta de uso exclusivo para os objetivos e funções de trabalho, o serviço de correio eletrônico corporativo, sendo proibida a sua utilização para outros fins.

§ 1º O endereço completo de e.mail terá a seguinte composição: "identificação do usuário @ domínio".

§ 2º A identificação do usuário, quando do cadastramento do usuário na rede do Ministério da Defesa, seguirá as orientações estabelecidas pela Secretaria de Logística e Tecnologia da Informação - SLTI, do Ministério do Planejamento, Orçamento e Gestão.

§ 3º O domínio adotado pelo Ministério da Defesa será "defesa.gov.br".

Art. 4º A Coordenação de Suporte da Divisão de Tecnologia da Informação – DIVTI deverá:

I - criar caixas postais departamentais, delegando privilégios para uso coletivo e caixas postais privadas, delegando privilégios a usuário específico;

II - designar permissões para acesso às caixas postais;

III - monitorar o acesso de usuários;

IV - estabelecer limites de espaço físico no servidor de dados para armazenamento de mensagens;

V - notificar os usuários, por meio de mensagens de alerta, quando as caixas postais excederem os limites de espaço estabelecidos, de modo que seus usuários eliminem ou transfiram seus conteúdos para pastas particulares criadas pelo próprio usuário na máquina local;

VI - manter a integridade e a disponibilidade do serviço de correio eletrônico e a recuperação de mensagens em caso de danos no ambiente;

VII - criar regras de filtragem, com o intuito de bloquear arquivos com possíveis códigos maliciosos e vírus; e

VIII - estabelecer e manter processo sistemático para gravação, retenção e destruição de mensagens de correio eletrônico.

Art. 5º A criação de caixas postais departamentais deverá ser solicitada à DIVTI, por meio de memorando, informando o nome dos usuários que a ela terão acesso e o responsável pela administração das mesmas.

Art. 6º A Coordenação de Apoio a Usuários em Informática é responsável pelo suporte à utilização do correio eletrônico.

Art. 7º Fica vedada:

I - toda e qualquer forma de utilização ou procedimento que não estiver explicitamente permitida nesta Instrução Normativa;

II - qualquer disseminação ou troca de informações com o meio externo à administração central do Ministério da Defesa sobre os conhecimentos, quer utilizados quer adquiridos no Ministério, salvo as situações expressamente autorizadas por autoridade competente, e

III - a tentativa de acesso não autorizado às caixas postais de terceiros, bem como o envio, não permitido, de informações críticas do Ministério para pessoas ou organizações.

Parágrafo único. Entende-se por conhecimento, utilizado ou adquirido no Ministério da Defesa, toda e qualquer mensagem de correio eletrônico corporativo referente a:

I - documentação de sistemas de informática (Códigos Fontes, Diagramas, Diagrama de Fluxos de Dados - DFD, Modelo Entidade Relacionamento - MER, Documentação de Tabelas, dentre outros);

II - propostas;

III - normas e procedimentos operacionais;

IV - projetos;

V - planos;

VI - documentos técnicos, sigilosos ou confidenciais; e

VII - quaisquer outros documentos e arquivos de interesse do Ministério da Defesa.

Art. 8º. Ensejará apuração de responsabilidade, conforme preceitua o art. 121 da Lei nº 8.112, de 11 de dezembro de 1990, o envio de documento eletrônico, cujo conteúdo se enquadre nas seguintes situações:

I - material obsceno, ilegal ou não ético;

II - propaganda ou mensagem, do tipo corrente ou entretenimento, relacionada com nacionalidade, raça, orientação sexual, religião, convicção política ou qualquer outro assunto que possa se constituir um ilícito penal;

III - material prejudicial à instituição, às suas parcerias, à sua imagem e aos seus servidores; e

IV - mensagens de cunho comercial e outros correlatos.

Art. 9º. A caixa postal do correio eletrônico corporativo será de propriedade do Ministério da Defesa, estando sob concessão de uso, podendo ser auditada, a qualquer tempo.

Art. 10. O envio simultâneo de mensagem ou envio de mensagens simultâneas a todos os usuários da rede, quando necessário, deverá ser efetuado por intermédio do Departamento de Administração Interna – DEADI ou pela Assessoria de Comunicação Social - ASCOM do Ministério da Defesa.

Art. 11. As mensagens enviadas pelas caixas postais departamentais terão, obrigatoriamente, a identificação do autor e do emissor, sendo imputada a este último as mesmas responsabilidades e atribuições de uma caixa postal privada de correio eletrônico corporativo.

Art. 12. A participação em listas de discussão, utilizando o serviço de correio eletrônico corporativo, será permitida somente quando o assunto for relacionado às atividades profissionais desenvolvidas pelo usuário no Ministério da Defesa.

Art. 13. Será observada a seguinte temporalidade para a utilização do endereço eletrônico corporativo:

I - durante o período de lotação do servidor ou da designação do militar na administração central do Ministério da Defesa; e

II - prazo determinado pela chefia imediata dos contratados de projetos, bolsistas, terceirizados e estagiários da administração central do Ministério da Defesa, respeitado o limite máximo de seis meses.

Parágrafo único. Ocorrendo desligamento de servidor em prazo inferior a seis meses, caberá à chefia imediata solicitar à DIVTI a exclusão do serviço de correio eletrônico corporativo.

Art. 14. As caixas postais de correio eletrônico corporativo disponibilizadas terão acesso exclusivamente interno, excetuando-se os casos descritos no art. 18 desta Instrução Normativa.

Art. 15. A exclusão do serviço de correio eletrônico corporativo se dará da seguinte forma:

I – os servidores lotados ou militares designados serão excluídos automaticamente, de acordo com a comunicação formal recebida da Divisão de Recursos Humanos – DIRHU, informando o desligamento dos mesmos; e

II – os contratados de projetos, os bolsistas, os terceirizados e os estagiários serão excluídos no prazo previsto no ato do cadastramento, podendo haver renovação do serviço, mediante solicitação expressa e justificada da chefia imediata.

Art. 16. O redirecionamento de mensagens recebidas em endereço eletrônico corporativo excluído, para outro endereço, será permitido somente para outra caixa de correio eletrônico corporativo, sendo que, para tal, deve haver manifestação formal e justificada da chefia imediata do solicitante.

Art. 17. Serão observados os seguintes limites máximos para definição dos tamanhos dos bancos de dados dos correio eletrônicos corporativos:

I - Ministro, Secretários e Chefe de Gabinete do Ministro – 200 Mb;

II - Chefes de Departamentos e Assessores Especiais – 150 Mb;

III - Gerentes – 100 Mb;

IV - Subgerentes, Coordenadores e Chefes de Seção – 80 Mb;

V - Demais servidores do MD – 50 Mb;

VI - contratados de projetos, bolsistas, terceirizados e os estagiários – 30 Mb; e

VII - caixas postais departamentais – 100 Mb.

Art. 18. O acesso à caixa de correio eletrônico do Ministério da Defesa por meio de redes externas – webmail – será permitido somente aos servidores lotados ou militares que ocupem as seguintes funções:

I - Ministro, Secretários e Chefe de Gabinete do Ministro;

II - Chefes de Departamentos e Assessores Especiais;

III – Gerentes; e

IV - Subgerentes, Coordenadores e Chefes de Seção.

Parágrafo unico. Os servidores lotados ou militares que ocupem as funções descritas nos incisos III e IV, deste artigo, somente terão o acesso quando expressamente solicitado pela chefia imediata.

Art. 19. Os arquivos transmitidos por e-mail devem ter o tamanho máximo de 10 Mb, caso haja necessidade de enviar arquivos maiores que o limite estabelecido, deve-se providenciar a compactação ou o fracionamento dos mesmos.

Art. 20. Os casos omissos serão resolvidos pelo Diretor do DEADI, ouvindo a DIVTI.

Art. 21. Esta Instrução Normativa entra em vigor na data de sua publicação.

ANTONIO CARLOS AYROSA ROSIÈRE

Anexo D

Documentos enviados como anexo pelo SERPRO

Serviço Federal de Processamento de Dados SERPRO

NORMA	IDENTIFICAÇÃO	VERSÃO	FOLHA (Nº/DE)
	SG/016	05	1/6

TÍTULO

USO SEGURO DE SERVIÇOS DE CORREIO ELETRÔNICO E MENSAGERIA

REFERÊNCIAS

TEMA: Segurança

PALAVRAS-CHAVE: correio, correio eletrônico, mensagem instantânea, mensageria

ANEXOS

VIGÊNCIA

INÍCIO: 01/11/2012 **FIM:**

1.0 FINALIDADE

Regulamentar os procedimentos sobre o uso seguro de serviços corporativos de correio eletrônico e mensageria.

2.0 ÂMBITO DE APLICAÇÃO

Todos os órgãos da Empresa.

3.0 DEFINIÇÕES

Para efeito desta Norma, entende-se por:

a) Caixa Postal Corporativa: caixa postal eletrônica, vinculada ao correio eletrônico, cujo endereço é destinado ao atendimento de mais de um usuário da mesma área ou com a mesma função, a fim de atender ao negócio da Empresa;

b) Caixa Postal Individual: caixa postal eletrônica, vinculada ao correio eletrônico, cujo endereço é destinado ao atendimento de um usuário, a fim de atender ao negócio da Empresa;

c) (A) Correio Eletrônico: tipo de correio disponível pelo SERPRO, de uso corporativo, por meio da Internet, que permite a comunicação entre usuários e dispõe de endereços postais eletrônicos cuja finalidade é identificar remetentes e destinatários;

Serviço Federal de Processamento de Dados SERPRO

NORMA	IDENTIFICAÇÃO	VERSÃO	FOLHA (Nº/DE)
	SG/016	05	2/6

TITULO

USO SEGURO DE SERVIÇOS DE CORREIO ELETRÔNICO E MENSAGERIA

d) (I) Correio Eletrônico Particular: tipo de correio eletrônico pessoal adquirido pelo usuário, onerosa ou gratuitamente, provido por terceiros e acessível por meio dos ativos informacionais do SERPRO;

e) *Email* Indesejado: mensagem recebida por meio de correio eletrônico, cujo teor é o desagravo pessoal, difamação, denúncia, pornografia, *e-mail phishing*, dentre outros;

f) *Email Phishing*: *email* falso que simula a identidade de entidades consideradas confiáveis com o objetivo de adquirir dados pessoais de diversos tipos: senha, conta bancária, número de cartão de crédito, dentre outros;

g) Estação de Trabalho: computador pessoal, ou qualquer outro equipamento que tenha recurso computacional equivalente, projetado para uso em mesa de trabalho e exclusivo para atividades da Empresa, podendo ser estação fixa ou estação móvel;

h) Mensagem Tipo Corrente: correspondência utilizada para replicar a mesma mensagem para muitas pessoas (malas diretas, pirâmides de enriquecimento fácil, ofertas tentadoras, abaixo-assinados);

i) Spam: termo usado para referir-se aos *emails* não solicitados, que geralmente são enviados para um grande número de pessoas; e

j) (A) Usuário: qualquer empregado, estagiário, adolescente aprendiz, contratado ou preposto contratado (terceirização), cliente ou fornecedor que detenha autorização para acesso e uso, por qualquer meio, aos ambientes de TIC do SERPRO.

4.0 DETERMINAÇÕES

4.1 **(A)** As caixas postais corporativas do correio eletrônico e seu conteúdo são de propriedade do SERPRO.

4.2 Uso de serviços corporativos de correio eletrônico e mensageria

4.2.1 O uso dos serviços corporativos de correio eletrônico e de mensageria instantânea é de responsabilidade do usuário e deve manter afinidade exclusiva com o objeto de seu

Serviço Federal de Processamento de Dados SERPRO

NORMA	IDENTIFICAÇÃO	VERSÃO	FOLHA (Nº/DE)
	SG/016	05	3/6

TITULO

USO SEGURO DE SERVIÇOS DE CORREIO ELETRÔNICO E MENSAGERIA

contrato de trabalho ou de prestação de serviços, inclusive em relação ao conteúdo de documentos, arquivos, trabalhos, mensagens, programas, imagens, vídeos e sons.

4.2.2 Todo empregado do SERPRO deve ser titular de uma única caixa postal individual no correio eletrônico corporativo, com direito de envio e recebimento de mensagens na Intranet e Internet.

4.2.3 **(A)** Cabe ao gestor de Unidade Organizacional decidir sobre a disponibilização de titularidade única de caixa postal do correio eletrônico corporativo do SERPRO para estagiário, adolescente aprendiz e empregado terceirizado, de empresa prestadora de serviço, contratada pelo SERPRO, com direito de envio e recebimento de mensagens na Intranet e Internet, enquanto perdurar o respectivo contrato.

4.2.3.1 **(A)** O gestor da Unidade Organizacional pode optar por caixa corporativa compartilhada, com identificação explícita de cada emissor, para estagiários, adolescentes aprendizes e empregados terceirizados, enquanto perdurar o respectivo contrato.

4.2.4 A Unidade Organizacional pode dispor de caixa postal corporativa compartilhada, em nome da Unidade, ficando a responsabilidade dessa caixa atribuída ao titular da Unidade ou grupo de usuário específico.

4.2.4.1 O titular da Unidade Organizacional, detentora de caixa postal corporativa compartilhada, deve designar um responsável pela administração dessa caixa e os usuários que terão acesso.

4.2.4.2 A caixa corporativa compartilhada pode identificar nominalmente o emissor por mensagem, facultando inclusive ao emissor enviar a mensagem em seu próprio nome.

4.3 Uso indevido de serviço de correio eletrônico e mensageria

4.3.1 São caracterizadas como utilização indevida de serviços de correio eletrônico e mensageria as seguintes ações:

a) **(A)** tentativa de acesso não autorizado à caixa postal de terceiros, de outros usuários ou ao conteúdo de mensagens alheias;

Serviço Federal de Processamento de Dados SERPRO

NORMA	IDENTIFICAÇÃO	VERSÃO	FOLHA (Nº/DE)
	SG/016	05	4/6

TITULO

USO SEGURO DE SERVIÇOS DE CORREIO ELETRÔNICO E MENSAGERIA

b) tentativa de acesso não autorizado a banco de dados do sistema de correio eletrônico corporativo;

c) **(A)** envio de informação classificada com grau de sigilo secreto, reservado, corporativo ou corporativo-legal, conforme Norma que trata sobre Classificação dos Ativos de Informação do SERPRO, para terceiros, para repositórios externos ou para organizações de qualquer natureza, sem prévia e expressa autorização de autoridade competente;

d) criação ou distribuição de material obsceno, ofensivo, ilegal ou não ético, propaganda, *spam* e mensagem tipo corrente;

e) criação ou distribuição de mensagem que cause molestamento, assédio ou tormento ao destinatário ou terceiros;

f) envio intencional de mensagem que contenha código malicioso ou qualquer forma de programa de computador prejudicial ou danosa;

g) utilização das listas públicas do SERPRO e de clientes para a distribuição de mensagens que não sejam de interesse funcional;

h) transmissão e retransmissão de mensagem com finalidade comercial de interesse particular ou para obtenção de ganho financeiro seja pessoal, benefício próprio ou de terceiros;

i) redirecionamento das caixas de correio eletrônico corporativo do SERPRO, da qual o usuário é o titular, para serviços de correio eletrônico de provedores externos; e

j) todo e qualquer procedimento de uso do correio eletrônico não previsto nesta Norma que possa afetar de forma negativa ou danosa o SERPRO, clientes e usuários.

4.4 Preservação de evidências de *email* indesejado

4.4.1 O usuário que receber *email* indesejado deverá tomar as seguintes providências:

a) manter o *email* indesejado em sua caixa de entrada e não repassar a outrem;

Serviço Federal de Processamento de Dados SERPRO

NORMA	IDENTIFICAÇÃO	VERSÃO	FOLHA (Nº/DE)
	SG/016	05	5/6

TITULO

USO SEGURO DE SERVIÇOS DE CORREIO ELETRÔNICO E MENSAGERIA

b) não abrir arquivo anexado ao *email* indesejado, uma vez que poderá conter código malicioso;

c) não confirmar o recebimento do *email*;

d) manter o conhecimento sobre a informação de forma restrita; e

e) registrar o evento, por meio de abertura de requisição de serviço do Processo SERPRO de Gestão Integrada de Serviços – PSGIS.

4.5 Os usuários devem ser conscientizados sobre como se proteger e contra o que se proteger no que se refere ao uso dos serviços de correio eletrônico e mensageria, de acordo com as necessidades identificadas pela área de segurança corporativa.

4.6 Todas as mensagens expedidas por correio eletrônico corporativo deve exibir os seguintes textos padrão de confidencialidade, de forma automática, a fim de minimizar o mau uso de correspondência extraviada ou redirecionada com malícia:

a) teor do texto em português - "Essa mensagem do SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO), empresa pública federal regida pelo disposto na Lei Federal nº 5.615, é enviada exclusivamente ao seu destinatário e pode conter informações confidenciais, protegidas por sigilo profissional. Sua utilização desautorizada é ilegal e sujeita o infrator às penas da lei. Se você a recebeu indevidamente, queira, por gentileza, reenviá-la ao emitente, esclarecendo o equívoco."; e

b) teor do texto em inglês - "*This message from SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO) - a government company stablished under Brazilian law (5.615/70) - is directed exclusively to its addressee and may contain confidencial data, protected under professional secrecy rules. Its unauthorized use is illegal and may subject the transgressor to the law´s penalties. If you´re not the addressee, please send it back, elucidating the failure.*".

5.0 DISPOSIÇÕES FINAIS

5.1 Os serviços de correio eletrônico e mensageria estão sujeitos à monitoração de acordo com a Norma que trata sobre Monitoração Eletrônica do Ambiente de TIC e suas Aplicações.

CANCELA A NORMA	VERSÃO	APROVAÇÃO	DATA
SG/016	04	Ulysses Alves de Levy Machado Coordenador Geral de Gestão da Segurança da Informação - COGSI	01/11/2012

Serviço Federal de Processamento de Dados SERPRO

NORMA	IDENTIFICAÇÃO	VERSÃO	FOLHA (Nº/DE)
	SG/016	05	6/6

TITULO

USO SEGURO DE SERVIÇOS DE CORREIO ELETRÔNICO E MENSAGERIA

5.2 **(A)** Poderá haver desabilitação de usuário dos serviços de correio eletrônico e mensageria do SERPRO diante de situações adversas, de acordo com os dispositivos desta Norma e das Normas que tratam sobre Monitoração Eletrônica do Ambiente de TIC e suas Aplicações e Desabilitação de Sistemas, Aplicativos e Ambientes.

5.3 A não observância destas determinações por parte do empregado da Empresa, sujeita o infrator às penalidades constantes das normas disciplinares do SERPRO, conforme decisão de autoridade competente, mediante recomendação de Comissão de Sindicância ou Processo Administrativo Disciplinar - PAD, constituído especialmente para aquele fim.

5.3.1 Cabe à Consultoria Jurídica orientar a Unidade Organizacional quando houver incidência de infração cometida por usuário não empregado do SERPRO.

5.4 **(I)** A monitoração do ambiente SERPRO, quando evidenciar a análise de conteúdo residente em Correio Eletrônico Particular, somente será feita mediante provocação da Consultoria Jurídica para obtenção de mandado judicial.

5.5 **(A)** Esta Norma está aderente ao Programa de Segurança do SERPRO - PSS e às Normas que tratam sobre Acesso Web, Monitoração Eletrônica do Ambiente de TIC e suas Aplicações, Classificação dos Ativos de Informação do SERPRO e Desabilitação de Sistemas, Aplicativos e Ambientes.

5.6 Os casos omissos serão tratados pela Coordenação-Geral de Gestão da Segurança da Informação junto às Superintendências responsáveis pela gestão do ambiente de correio eletrônico.

Anexo E

Documentos enviados como anexo pelo Ministério da Comunicação

SECRETARIA-EXECUTIVA

SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO

PORTARIA Nº 1410/2014/SEI-MC

de 18 de setembro de 2014

O PRESIDENTE DO COMITÊ DE TECNOLOGIA E DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, no uso das atribuições legais definidas pela Portaria 1018/2014/SEI-MC, de 25 de Agosto de 2014; e

Considerando os termos da Instrução Normativa nº 01/GSI/PR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta;

Considerando a Norma Complementar nº 03/DSIG/GSIPR, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações - PoSIC nos órgãos e entidades da Administração Pública Federal, direta e indireta;

Considerando os termos do Decreto nº 3.505 de 13 de junho de 2000, que institui a Politica de Segurança da Informação nos órgãos e entidades da administração Pública Federal; e,

Tendo em vista o que consta do processo nº 53900.010646/2014-21,

RESOLVE:

Art. 1º Atualizar a Política de Segurança da Informação e Comunicações - PoSIC no âmbito do Ministério das Comunicações, na forma do Anexo I a esta portaria.

Art. 2º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço.

Art. 3º Ficam revogadas a Portaria SPOA nº 500 de 26 de novembro de 2012, Portaria SPOA nº 519 de 13 de dezembro de 2012 e a Portaria SPOA nº 518 de 13 de dezembro de 2012.

ULYSSES CESAR AMARO DE MELO
Presidente do Comitê de Tecnologia e de Segurança da Informação e Comunicações

ANEXO I

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES – PoSIC

Art. 1° O presente documento tem por objetivo atualizar a Política de Segurança da Informação e Comunicações – PoSIC no âmbito do Ministério das Comunicações.

Capítulo I
ESCOPO

Seção I
Diretrizes Gerais

Art. 2° A PoSIC objetiva garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pelo MC, observando-se os princípios e as diretrizes estabelecidas na Lei de Acesso a Informação (Lei n° 12.527, de 18 de novembro de 2011).

Art. 3° Integram também a PoSIC as normas e os procedimentos destinados à proteger e disciplinar o uso da informação.

Art. 4° As diretrizes de Segurança da Informação e Comunicações - SIC devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais e estrutura do MC, além dos princípios de transparência.

Art. 5° O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado por meio de verificações de conformidade.

Art. 6° É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo MC.

Art. 7° Os recursos tecnológicos, as instalações de infraestrutura, sistemas de informação e as aplicações devem ser protegidos, no que couber, contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 8° Fica nomeado o Coordenador-Geral de Tecnologia da Informação como Gestor de Segurança da Informação e Comunicações.

Art. 9° Fica instituída a Equipe de Tratamento de Incidentes e Resposta a Ataques na Rede MC – ETIR, vinculada a Subsecretaria de Planejamento, Orçamento e Administração – SPOA.

§ 1° A autonomia da ETIR será completa, podendo tomar às ações necessárias para reforçar a resposta ou a postura do MC na recuperação de incidentes de segurança sem esperar pela aprovação de níveis superiores de gestão.

§ 2° A ETIR será composta por servidores públicos designados em portaria específica do Gestor de Segurança da Informação e Comunicações.

Seção II
Abrangência

Art. 10. As diretrizes, normas complementares e manuais de procedimentos da PoSIC do MC aplicam-se a servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a aqueles que, de alguma forma, executem atividades vinculadas ao MC.

§ 1° Os contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo MC devem atender, no que couber, a esta PoSIC e demais normas relacionadas.

§ 2° Esta política também se aplica, no que couber, ao relacionamento do MC com outros órgãos e entidades públicos ou privados.

Capítulo II
CONCEITOS E DEFINIÇÕES

Art. 11. Para o disposto nesta PoSIC, consideram-se as seguintes definições:

I - acesso remoto: funcionalidade que permite acesso ao conteúdo ou controle de um determinado computador através da internet;

II - agente responsável pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal - APF incumbido de chefiar e gerenciar a ETIR;

III - ameaça: evento que tem potencial em si próprio para comprometer os objetivos da organização, seja trazendo danos diretos aos ativos ou prejuízos decorrentes de situações inesperadas;

IV - ativos de informação: os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

V - autenticidade: garantia de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

VI - capacitação em SIC: atividade de ensino e aprendizagem sobre temas relacionados à segurança da informação e comunicações;

VII - classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;

VIII - Comitê de Tecnologia e Segurança da Informação e Comunicações - CTSIC: colegiado de caráter deliberativo responsável pela normatização e supervisão da segurança da informação e comunicações no âmbito do MC;

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

X - conscientização em SIC: saber o que é segurança da informação e

comunicações aplicando em sua rotina pessoal e profissional, além de servir como multiplicador sobre o tema;

XI - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

XII - CTIR.GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República - DSIC/GSI/PR;

XIII - custodiante do ativo de informação: é 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;

XIV - disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade;

XV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: colegiado com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no âmbito do MC;

XVI - gestão de ativos: processo sistemático de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XVII - 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. Esse processo fornece 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;

XVIII - gestão de riscos de segurança da informação e comunicações - GRSIC: 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;

XIX - Gestor de SIC: servidor nomeado pelo Ministro de Estado como responsável pela gestão de segurança da informação e comunicações no âmbito do MC;

XX - incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXI - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

XXII - infraestrutura de TI: instalações prediais (energia, água, climatização, acesso físico), computadores e equipamentos, software, redes e telecomunicações, sistemas de armazenamento e recuperação de dados (arquivos e armazenamento), aplicações computacionais, cabeamento e rede telefônica;

XXIII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXIV - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

XXV - recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

XXVI - risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XXVII - segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

XXVIII - sensibilização em SIC: saber o que é segurança da informação e comunicações aplicando em sua rotina pessoal e profissional;

XXIX - terceiros: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao MC;

XXX - tratamento de incidentes: é o 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;

XXXI - usuário: servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e a quem, de alguma forma, execute atividades vinculadas a este Ministério;

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

Capítulo III
DIRETRIZES ESPECÍFICAS

Art. 12. Para cada uma das diretrizes constantes das seções deste capítulo podem ser elaboradas normas específicas, manuais e procedimentos, aprovados e publicadas pelo CTSIC.

Seção I
Da Gestão de Ativos da Informação

Art. 13. Os ativos de informação devem:

I - ser inventariados e protegidos;

II - ter identificados os seus proprietários e custodiantes;

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

IV - ter entrada e saída nas dependências do MC autorizadas e registradas por autoridade competente;

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 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, observando a legislação em vigor.

Art. 14. Norma específica deve estabelecer os critérios de tratamento e

classificação da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Seção II
Da Gestão de Riscos

Art. 15. Norma específica deve estabelecer processos que possibilitarão identificar ameaças e reduzir vulnerabilidades e impactos dos ativos de informação.

Seção III
Da Segurança Física e do Ambiente

Art. 16. Norma específica deve estabelecer mecanismos de proteção para as instalações físicas e para as áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências, em resposta aos riscos identificados.

Seção IV
Da Segurança em Recursos Humanos

Art. 17. Todos os usuários devem observar, difundir e exigir o cumprimento da PoSIC, das normas de segurança e da legislação vigente acerca do tema.

Art. 18. Norma específica deve estabelecer processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os usuários, de acordo com suas competências funcionais.

Seção V
Da Gestão de Operações e Comunicações

Art. 19. A Coordenação Geral de Tecnologia da Informação - CGTI 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.

Seção VI
Dos Controles de Acessos

Art. 20. Eventos relevantes, previamente definidos, devem ser registrados para a segurança e o rastreamento de acesso às informações.

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

Art. 21. A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando que as atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário dependem de prévia autorização do gestor da área responsável pela informação.

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

§ 2° Os usuários são responsáveis por todos os atos praticados com suas identificações, tais como: nome de usuário, senha, crachá, carimbo, correio eletrônico, assinatura digital e recursos criptográficos.

§ 3º 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.

§ 4º Todos os sistemas de informação do MC devem ter um gestor, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações, conforme definido em norma específica.

Art. 22. É vedada a utilização de acesso remoto, salvo utilização de recursos próprios do Ministério, homologados pela CGTI.

Seção VII
Da Criptografia

Art. 23. Norma específica deve estabelecer parâmetros para o uso de recursos criptográficos no MC.

Art. 24. O usuário é responsável pelo recurso criptográfico que receber, devendo assinar Termo de Responsabilidade pelo seu uso.

Seção VIII
Da Aquisição, do Desenvolvimento e da Manutenção de Sistemas

Art. 25. A CGTI deve estabelecer critérios de segurança para o desenvolvimento, manutenção e aquisição de sistemas e aplicações.

Seção IX
Do Tratamento de Incidentes

Art. 26. Norma específica deve estabelecer processo de gestão para tratamento e respostas a incidentes de segurança, de forma a observar o disposto em normativos do CTIR.GOV.

Seção X
Da Gestão de Continuidade

Art. 27. Norma específica deve estabelecer parâmetros para a gestão de continuidade do negócio.

Seção XI
Da Conformidade

Art. 28. Deve ser realizada, com periodicidade mínima anual, verificação de conformidade das práticas de SIC do MC e de suas unidades administrativas em relação à esta PoSIC e suas normas complementares, bem como em relação à legislação específica de SIC.

§ 1º A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com o MC.

§ 2º A verificação da conformidade será realizada conforme calendário

elaborado com base na priorização dos riscos identificados ou percebidos e aprovado pelo CTSIC.

§ 3º A verificação de conformidade será executada pelo Gestor de SIC, podendo para compor grupo de trabalho específico ou subcontratar o serviço no todo ou em parte.

§ 4º É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

§ 5º Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Gestor de SIC ao Gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

Seção XII
Do Plano de Investimentos em SIC do MC

Art. 29. Os investimentos em SIC serão planejados com base nos riscos identificados e consolidados no Plano Diretor de Tecnologia da Informação – PDTI, aprovado pelo CTSIC.

Seção XIII
Da Propriedade Intelectual

Art. 30. As informações produzidas por usuários, no exercício de suas funções, são patrimônio intelectual do MC e não cabe a seus criadores qualquer forma de direito autoral.

Art. 31. Nos termos da Lei de Acesso a Informação (Lei nº 12.527, de 18 de novembro de 2011), é vedada a divulgação e uso por terceiros de informações restritas ou classificadas por grau de sigilo, produzidas ou custodiadas pelo MC, salvo nos casos de autorização específica.

Parágrafo único. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre informações de terceiros antes de seu uso.

Seção XIV
Dos Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 32. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIC e demais normas relacionadas.

§ 1º Os contratos, convênios, acordos e instrumentos congêneres que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pelo MC.

§ 2º Os contratos, convênios, acordos e instrumentos congêneres devem conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem.

§ 3º Os contratos, convênios, acordos e instrumentos congêneres devem prever a obrigação de divulgação desta PoSIC 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.

Seção XV
Da Gestão de Mudanças

Art. 33. Norma específica deve estabelecer processo de gestão de mudanças.

Capítulo IV
PENALIDADES

Art. 34. Ações que violem a PoSIC ou quaisquer de suas diretrizes, normas e procedimentos ou que quebrem os controles de SIC serão devidamente apuradas e aos responsáveis serão aplicadas as sanções administrativas, cíveis e penais em vigor.

Capítulo V
COMPETÊNCIAS E RESPONSABILIDADES

Art. 35. Cabe ao Gestor de Segurança da Informação e Comunicações (SIC):

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 SIC;

IV - designar membros e coordenar a ETIR;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

VI - manter contato direto com o DSIC/GSI/PR para o trato de assuntos relativos à segurança da informação e comunicações; e

VII - propor normas relativas à SIC.

Art. 36. Cabe ao Agente responsável pela ETIR:

I - Coordenar e acompanhar:

a) As atividades de tratamento e resposta a incidentes nas redes computacionais deste Ministério;

b) A análise dos sistemas comprometidos buscando, causas, danos e responsáveis;

c) A avaliação, auditoria e testes das condições de segurança das redes computacionais deste Ministério;

d) A análise dos ativos de informação e estruturas constitutivas dos ambientes de tecnologia da informação, presentes neste Ministério;

II - Coordenar, acompanhar e orientar as equipes no reparo a danos causados por incidentes de segurança;

III - Executar outras atividades correlatas que lhe forem demandadas;

IV - Participar, juntamente com o Gestor de Segurança da Informação e

Comunicações, na proposição de recursos necessários às ações de segurança da informação e comunicações;

V - Manter em condições adequadas de segurança o acervo de informações relativas aos incidentes nas redes computacionais do Ministério;

VI - Participar da definição e acompanhar os indicadores de acompanhamento de incidentes nas redes computacionais do Ministério;

VII - Prestar assessoria técnica na elaboração de políticas, normas, pareceres e na especificação técnica de produtos e equipamentos direcionados à segurança da informação e comunicações;

VIII - Planejar, coordenar, supervisionar e orientar a execução das atividades da respectiva unidade;

IX - Assistir o CTIR GOV com as informações necessárias à atualização e manutenção das bases de dados de incidentes do Governo Federal;

X - Assistir à autoridade competente nos assuntos pertinentes à sua área de atuação; e

XI - Desenvolver um Plano de Conscientização em segurança da informação e comunicações a fim de que todos os servidores do MC tenham ciência do assunto.

Art. 37. Cabe à ETIR:

I - Garantir a segurança da informação e comunicações no âmbito do Ministério das Comunicações, por meio do estrito cumprimento da PoSIC, suas normas e da gestão de riscos continuada;

II - Facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais;

III - Promover a recuperação de sistemas;

IV - Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança e, avaliando condições de segurança de redes por meio de auditorias;

V - Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

VI - Analisar ataques e intrusões na rede MC;

VII - Estabelecer regras para ações disciplinatórias no caso de condutas que violem as políticas estabelecidas ou que comprometam a segurança das informações da organização;

VIII - Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, as causas, a data de ocorrência, a sua frequência e os custos resultantes;

IX - Cooperar com outras equipes de Tratamento e Resposta a Incidentes computacionais; e

X - Participar em fóruns, redes nacionais e internacionais relativos à SIC.

Art. 38. Cabe ao titular da unidade administrativa:

I - responsabilizar-se pelas ações realizadas por aqueles usuários que estão sob

sua supervisão;

II - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de SIC;

III - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à SIC;

IV - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da SIC por parte dos usuários sob sua supervisão;

V - informar à CGGP/SPOA/SE a movimentação de pessoal de sua unidade;

VI - realizar o tratamento e a classificação da informação;

VII - autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

VIII - comunicar à ETIR os casos de quebra de segurança; e

IX - manter lista atualizada dos ativos de informação sob sua responsabilidade com seus respectivos gestores.

Art. 39. Cabe aos terceiros e fornecedores, conforme previsto em contrato:

I - tomar conhecimento desta PoSIC;

II - fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e

III - fornecer toda a documentação dos sistemas, produtos, serviços relacionados às suas atividades.

Art. 40. Cabe aos usuários:

I - conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PoSIC, bem como os demais normativos e resoluções relacionados à SIC;

II - obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e

III - comunicar os incidentes que afetam a segurança dos ativos de informação e comunicações à ETIR.

Capítulo VI
ATUALIZAÇÃO

Art. 41. Esta PoSIC poderá ser revisada a qualquer tempo por deliberação do CTSIC.

Documento assinado eletronicamente por **Ulysses Cesar Amaro de Melo**, **Subsecretário de Planejamento, Orçamento e Administração**, em 18/09/2014, às 17:31, conforme art. 3°, III, "a", da Portaria MC 89/2014.
N° de Série do Certificado: 667116279323853588469077018895734664 24

SUBSECRETARIA DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO

NORMA OPERACIONAL Nº SEI-MC 8

De 28 de novembro de 2014.

Estabelece os procedimentos para o uso dos recursos de Tecnologia da Informação e Comunicação no âmbito do Ministério das Comunicações. Revoga a Norma Operacional 006/2014/SEI-MC, de 08 de agosto de 2014.

O PRESIDENTE DO COMITÊ DE TECNOLOGIA E DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES, no uso de suas atribuições e da competência que lhe foi atribuída no inciso IV, art. 1°, da Portaria 1018/2014/SEI-MC, de 25 de agosto de 2014 e publicada no DOU do dia 1° de setembro de 2014, resolve:

Art. 1° Estabelecer, na forma dos seus anexos, os procedimentos para o uso dos recursos de Informática e Tecnologia da Informação e Comunicação (TIC) no âmbito do Ministério das Comunicações (MC).

I – Anexo I – Do cadastramento, alteração e desligamento de usuários dos serviços

II – Anexo II – Do uso das estações de trabalho

III – Anexo III – Do serviço de rede de comunicação de dados

IV – Anexo IV – Do serviço de correio eletrônico

V – Anexo V – Do serviço de telefonia fixa e móvel

Art. 2° Esta Norma aplica-se a todos que utilizam os serviços de TIC no âmbito do MC, aqui denominados usuários, assim relacionados.

I - Servidor público de provimento efetivo, temporário ou de livre nomeação-exoneração, gerido pela Coordenação-Geral de Gestão de Pessoas;

II - Prestador de serviço contratados ou cedidos por meio de acordo de cooperação técnica, gerido pelos respectivos gestores de contratos;

III - Estagiário contratado por meio de termo específico, gerido pela Coordenação-Geral de Gestão de Pessoas;

IV - Colaborador eventual que realize atividades em caráter temporário e necessite o uso de recursos de TIC, gerido por servidor de função DAS 4 ou superior na estrutura do MC.

Art. 3° A solicitação de suporte aos serviços constantes nesta norma deverão ser realizados diretamente à Coordenação-Geral de Tecnologia da Informação - CGTI, por meio dos seguintes canais de atendimento:

I – Sistema de atendimento disponível na intranet

II – Ramal: 6070

III – Email: suporte@comunicacoes.gov.br

Art. 4° A inobservância dos dispositivos constantes nesta norma sujeitará o infrator aos pertinentes procedimentos administrativos, com vistas a eventual aplicação de penalidades.

Art. 5° Revoga-se a Norma Operacional 006/2014/SEI-MC, de 08 de agosto de 2014.

Art. 6° Esta Norma Operacional entra em vigor na data de sua publicação em Boletim de Serviço.

ULYSSES CESAR AMARO DE MELO

ANEXO I

DO CADASTRAMENTO, ALTERAÇÃO E DESLIGAMENTO DE USUÁRIOS DOS SERVIÇOS

1. OBJETIVO

Regulamentar os critérios e procedimento para cadastramento, alteração e desligamento de usuários dos serviços de tecnologia da informação e comunicações no MC.

2. DO CADASTRO

2.1. O cadastro de usuário para servidor, prestador de serviço e estagiário nos serviços de TIC deverá ser precedido de cadastro do colaborador no Sistema de Recursos Humanos (SRH), por meio do seu gestor, conforme Art. 2°

2.2. A partir do cadastro no SRH a CGTI fará automaticamente a criação de usuário para acesso aos serviços de TIC e a criação de endereço de correio eletrônico para o usuário.

2.3. O cadastro de usuário para colaborador eventual deverá ser solicitado por servidor ocupante de DAS 4 ou superior a partir do formulário "Cadastro de Usuário como Colaborador Eventual" presente no Sistema Eletrônico de Informação (SEI) e será obrigatoriamente de duração temporária.

3. DA ALTERAÇÃO

3.1. A alteração nos dados dos usuários para servidor, prestador de serviço e estagiário deverá ser realizada por meio do próprio usuário ou de seu gestor diretamente no sistema SRH.

3.2. No caso de alteração da unidade de lotação e/ou exercício do usuário, o SRH deverá informar a CGTI eletronicamente desta mudança. A CGTI removerá todos os acessos do usuário aos sistemas em que estiver vinculado, a exceção dos sistemas SRH e de Ponto Eletrônico, este último para o caso de usuário do tipo servidor.

3.3. Os gestores de sistema ou sítio serão responsáveis por conceder acessos a sistemas necessários às atividades do usuário na nova unidade de lotação ou exercício do usuário.

4. DO DESLIGAMENTO

4.1. É de responsabilidade do gestor do usuário registrar imediatamente o seu desligamento do MC, a partir do sistema SRH.

4.2. A partir da informação do seu desligamento, a CGTI fará automaticamente o bloqueio do usuário, impedindo-o de utilizar os serviços de TIC do MC.

4.3. Através de rotina diária, a CGTI fará bloqueio de usuários com cadastro de duração temporária ou com mais de 35 dias corridos sem login nos serviços de rede e de correio eletrônico, exceto para usuários em situação de licença no sistema SRH.

4.4. A CGTI fará a exclusão definitiva do usuário após 10 dias corridos do seu bloqueio, precedida de cópia de segurança (*backup*) das informações de interesse do MC.

5. DOS PERFIS DE USUÁRIOS

5.1. O acesso e o limite de uso aos serviços de tecnologia da informação e comunicação serão regidos de acordo com o perfil do usuário.

5.2. Os perfis de usuários dos serviços de TIC são os seguintes:

Tabela 1 - Relação de perfis de usuários

Perfil	**Usuários atribuídos por padrão ao perfil**
A1	Servidores NE ou DAS 6
A2	Servidores DAS 5
A3	Servidores DAS 4
B1	Servidores DAS 3
B2	Servidores DAS 2 ou 1
B3	Demais servidores
C1	Prestadores de serviço ou Colaboradores eventuais

C2	Estagiários
E1	Secretárias - Apoio administrativo dos gabinetes
E2	Usuários móveis - Usuários que requerem recursos de mobilidade para a realização do seu trabalho

5.3. A inclusão de usuários nos perfis especiais é realizada individualmente, sendo necessário:

- Perfil E1: no mínimo que a solicitação seja enviada por Coordenador-Geral ou equivalente, sob sua gestão hierárquica;
- Perfil E2: no mínimo que a solicitação seja enviada por Diretor ou equivalente, sob a sua gestão hierárquica.

5.4. A alteração do perfil de um usuário poderá ser realizada, desde que devidamente justificada, partir do formulário "Mudança de Perfil ou Acesso de Usuário" no SEI por Coordenador-Geral, equivalente ou superior sob a sua gestão hierárquica. O novo perfil será no máximo igual ao perfil do usuário responsável pela solicitação.

5.5. Os usuários atribuídos a cada perfil deverão ter disponíveis os seguintes serviços:

Tabela 2 - Recursos de rede disponíveis por perfil de usuário

Perfil	**Rede Intranet**	**Rede Wifi - Produção**	**Rede VPN[1]**
A1	X	X	X
A2	X	X	X
A3	X	X	X
B1	X	X	
B2	X	X	
B3	X	X	
C1	X	X	
C2	X	X	
E1	X	X	

E2	X	X	X

[1] Acesso individual ao recurso poderá ser concedido para usuários mediante formulário "Mudança de Perfil ou Acesso de Usuário" no SEI por Coordenador-Geral ou equivalente e aprovação da CGTI.

Tabela 3 - Recursos de rede Internet disponíveis por perfil de usuário

Perfil	**Rede Internet[1]**					
	Demais conteúdos	**Redes sociais[2]**	**Compart. e sincronização de arquivos**	**Portais de download de arquivos**	**Webmail pessoal[2]**	**Streaming de mídia[2]**
A1	X	-	-	-	X	X
A2	X	-	-	-	X	X
A3	X	-	-	-	X	X
B1	X	-	-	-	X	X[3]
B2	X	-	-	-	X	X[3]
B3	X	-	-	-	X	X[3]
C1	X	-	-	-	-	-
C2	X	-	-	-	-	-
E1	X	-	-	-	-	-
E2	X	-	-	-	X	X

[1] Acesso individual ao recurso poderá ser concedido para usuários mediante formulário "Mudança de Perfil ou Acesso de Usuário" no SEI por Coordenador-Geral ou equivalente e aprovação da CGTI.

[2] Acesso ao recurso concedido à todos os usuários durante o intervalo de almoço (12:00 às 14:00).

[3] Acesso ao recurso concedido com restrição velocidade de banda.

Tabela 4 - Recursos de dispositivos disponíveis por perfil de usuário

Perfil	Softwares	Mobilidade	Estação de trabalho		
	Pacote Padrão	Tablet[2]	Notebook[2]	Desktop	Qtd Monitores[1]
A1	X	X	X	-	1
A2	X	X	X	-	1
A3	X	-	-	X	1
B1	X	-	-	X	1
B2	X	-	-	X	1
B3	X	-	-	X	1
C1	X	-	-	X	1
C2	X	-	-	X	1
E1	X	-	-	X	1
E2	X	X	X	-	1

[1] Acesso individual ao recurso poderá ser concedido para usuários mediante formulário "Mudança de Perfil ou Acesso de Usuário" no SEI por Coordenador-Geral ou equivalente e aprovação da CGTI.

[2] Acesso individual ao recurso poderá ser concedido para usuários mediante formulário "Mudança de Perfil ou Acesso de Usuário" no SEI por Diretor ou equivalente e aprovação da CGTI.

Tabela 5 - Recursos de correio eletrônico por perfil de usuário

Perfil	Correio Eletrônico		

	Disponível	Limite de Caixa	Limite de Armazenamento Remoto
A1	X	10Gb	10Gb
A2	X	10Gb	10Gb
A3	X	10Gb	10Gb
B1	X	500Mb	3Gb
B2	X	500Mb	3Gb
B3	X	500Mb	3Gb
C1	X	500Mb	3Gb
C2	X	500Mb	3Gb
E1	X	500Mb	3Gb
E2	X	10Gb	10Gb

Tabela 6 - Recursos de telefonia fixa por perfil de usuário

Perfil	**Telefonia Fixa**					
	Telefone	**Local**	**DDD**	**DDI**[1]	**Celular**	**Limite**
A1	IP - Videofone	X	X	X	X	Ilimitado
A2	IP - Videofone	X	X	X	X	R$ 150,00
A3	IP - Videofone	X	X	-	X	R$ 100,00
B1	IP - Normal	X	X	-	X	R$ 100,00

B2	IP - Normal	X	X	-	X	R$ 100,00
B3	IP - Normal	X	X	-	X	R$ 100,00
C1	IP - Normal	X	X	-	X	R$ 100,00
C2	IP - Normal	X	-	-	-	R$ 100,00
E1	IP - Normal	X	X	X	X	R$ 200,00
E2	IP - Normal	X	X	-	X	R$ 100,00

[1] Acesso individual ao recurso poderá ser concedido para usuários mediante formulário "Mudança de Perfil ou Acesso de Usuário" no SEI por Diretor ou equivalente e aprovação da CGTI.

Tabela 7 - Recursos de telefonia móvel por perfil de usuário

Perfil	**Telefonia Móvel**			
	Telefone	**Voz e Dados Nacional**	**Voz e Dados Internacional**	**Limite**
A1	Smartphone	X	Permanente	Ilimitado
A2	Smartphone	X	Temporário	R$ 450,00
A3	Smartphone	X	Temporário	R$ 300,00
B1	NA	-	-	NA
B2	NA	-	-	NA
B3	NA	-	-	NA
C1	NA	-	-	NA
C2	NA	-	-	NA

E1	NA	-	-	NA
E2	Smartphone	X	Temporário	R$ 300,00

6. DA REGRA DE CRIAÇÃO DE NOME DE USUÁRIO (*LOGIN*)

6.1. As regras de formação de nomes de usuários tem como base a padronização aprovada pela Worldwide Electronic Messaging Association-WEMA conforme padrões internacionais definidos pela ITU-International Telecommunications Union / Telecommunication Standardization Sector.

6.2. A identificação de uma pessoa é formada por pelo menos um nome e um sobrenome e pode conter nome(s) e sobrenome(s) intermediário(s).

- Exemplo: **Joaquim José da Silva Xavier**

6.3. Para efeito de formação, o nome do usuário é decomposto em três partes:

- PRENOME (ou primeiro nome): **JOAQUIM**
- NOME(S) INTERMEDIÁRIO(S): **JOSÉ DA SILVA**
- SOBRENOME (ou último nome): **XAVIER**

6.4. O nome do usuário deverá ter, sempre que possível, a forma mais simples, isto é, PRENOME seguido de um PONTO (.) seguido do SOBRENOME:

- **JOAQUIM.**XAVIER

6.5. No caso da existência de um usuário homônimo cadastrado, é necessário que o nome do novo usuário contenha um elemento que o diferencie do anterior. As alternativas são:

- Incluir a(s) inicial(is) do(s) nome(s) intermediário(s):
  - **joaquim.j.xavier ou**
  - **joaquim.s.xavier ou**
  - **joaquim.js.xavier ou**
- Formar prenome ou sobrenome compostos, usando o hífen para juntá-los:
- **joaquim-jose.xavier ou**
- **joaquim.silva-xavier ou**
- **joaquim-jose.silva-xavier ou**
- **joaquim-jose.s.xavier ou**
- **joaquim.j.silva-xavier ou**
- **joaquim-jose.da-silva-xavier**

6.6. Porém, algumas restrições deverão ser observadas:

- Não utilizar acentos (til, agudo, grave, circunflexo, trema):
- PRENOME, simples ou composto, pode ter no máximo 16 caracteres, permitidos caracteres alfabéticos, maiúsculos ou minúsculos, e hífen, sem espaços entre eles.
- INICIAIS dos nomes intermediários – máximo de três caracteres, permitidos caracteres alfabéticos, maiúsculos ou minúsculos, hífen e ponto, sem espaços entre eles.
- SOBRENOME, simples ou composto, pode ter no máximo 40 caracteres, permitidos caracteres alfabéticos, maiúsculos ou minúsculos, e hífen, sem espaços entre eles.

- Quando constarem do sobrenome qualificadores de geração (Júnior, Filho, Neto e outros), é recomendável usar o sobrenome composto:
  - JOAQUIM.J.XAVIER-FILHO

ANEXO II

DO USO DAS ESTAÇÕES DE TRABALHO

1. OBJETIVO

Regulamentar a utilização dos equipamentos de hardware e software, aqui denominados estações de trabalho, disponibilizados aos usuários dos serviços de TIC do MC.

2. UTILIZAÇÃO DAS ESTAÇÕES DE TRABALHO

2.1. As estações de trabalho destinam-se preferencialmente ao uso dos usuários do tipo servidores.

2.2. Todos os usuários, exceto os de perfil visitante e público, farão jus a uma estação de trabalho enquanto perdurar o contrato ou serviço específico.

2.3. O usuário que necessitar de acesso administrador na sua estação de trabalho, deverá solicitar mediante formulário "Acesso de Usuário como Administrador de Computador" no SEI por Coordenador-Geral ou equivalente e aprovação da CGTI.

3. OBRIGAÇÕES DO USUÁRIO

3.1. São obrigações do usuário de uma estação de trabalho:

- Manter o padrão de configuração de hardware e software das estações de trabalho estabelecido pela CGTI. Sendo permitida apenas à CGTI realizar alterações nestas configurações;
- Manter a estação de trabalho em local seguro e arejado;
- Evitar consumo ou armazenamento de bebidas e comidas próximo à estação de trabalho;
- Manter limpo o local onde a estação de trabalho está locada;
- Manter a segurança de seus arquivos.
- Desligar ou bloquear o equipamento em caso de afastamento;
- Acionar a CGTI sempre que houver problemas técnicos com a estação de trabalho ou sua configuração;
- Desligar a estação de trabalho ao final do expediente.

4. USO INDEVIDO DAS ESTAÇÕES DE TRABALHO

4.1. No uso das estações de trabalho são vedadas as seguintes ações:

- Expor a estação de trabalho a choques, interferências elétricas ou magnéticas, utilização de líquido corrosivo ou não e outras ações que possam provocar danos à mesma;
- Instalar ou alterar a configuração de hardware da Estação de Trabalho, sem a devida autorização da CGTI;
- Utilizar a estação de trabalho em atividades particulares com fins lucrativos;
- Abrir ou violar a estação de trabalho, para qualquer finalidade, sem a devida autorização da CGTI.
- Manter na estação de trabalho material obsceno, ofensivo, ilegal ou antiético, comercial privado ou que incentive ou instrua a invasão de equipamentos de informática;

- Copiar ou transmitir a terceiros, sem autorização prévia, dados, informações, programas de computador, procedimentos, instruções, controles e listas de endereços de correio eletrônico pertencentes ao MC;

5. UTILIZAÇÃO DOS PROGRAMAS DE COMPUTADOR (*SOFTWARES*)

5.1. Os softwares adquiridos ou desenvolvidos no âmbito do MC, instalados nas estações de trabalho, descritos aqui simplesmente como softwares, são de propriedade e responsabilidade deste ministério.

5.2. A instalação de softwares nas estações de trabalho ou outros dispositivos será precedida da homologação dos mesmos pela equipe da CGTI.

5.3. É vedada qualquer instalação de software nas estações de trabalho que não tenha sido previamente homologado pela CGTI.

5.4. Os softwares somente poderão ser instalados pela CGTI, sendo vedada a instalação e alteração por parte dos usuários, exceto quando autorizado pela CGTI.

5.5. Os programas de computador (*softwares*) de propriedade de terceiros instalados nas estações de trabalho também são de responsabilidade do MC, os quais deverão acompanhar seus contratos específicos formalizados ou o seu termo de responsabilidade, juntamente com o comprovante da chave de registro do produto.

5.6. No uso de softwares dentro do ambiente do MC são vedadas as seguintes ações:

- Gerar, compilar, copiar, propagar, executar ou tentar introduzir em estações de trabalho ou sistemas do MC códigos maliciosos ou softwares contendo processos destrutivos de espionagem ou propaganda;
- Utilizar softwares para invasão de equipamentos e ou sistemas do MC ou de seus servidores, com exceção das situações motivadas e aprovadas pela CGTI;
- Utilizar softwares de propriedade do MC em atividades particulares com fins lucrativos.

ANEXO III

DO SERVIÇO DE REDE DE COMUNICAÇÃO DE DADOS

1. OBJETIVO

Regulamentar os critérios e procedimentos para utilização dos serviços de acesso à rede digital de comunicação de dados do MC, a partir dos perfis dos usuários.

2. REDE LOCAL

2.1. A utilização da rede local engloba desde o login, senhas, manutenção de arquivos em servidores, ao acesso a serviços diversos como correio eletrônico e sistemas departamentais e corporativos.

2.2. São regras para a utilização da rede local:

- O usuário é o responsável pelo uso e pela segurança de sua conta de acesso, devendo seu nome de usuário e sua senha serem tratados de forma privada e confidencial, não devendo ser compartilhada com terceiros. A conta de acesso e os recursos e privilégios dela advindos são

intransferíveis, sendo de inteira responsabilidade do usuário toda e qualquer consequência advinda de utilização indevida;
- Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas. Deverá, também, efetuar o logout / logoff da rede ou o bloqueio da estação de trabalho, sendo inteira responsabilidade do usuário toda e qualquer consequência advinda de utilização indevida.

2.3. Acesso às pastas públicas localizadas nos servidores de arquivo:

- Caso uma área julgue conveniente, poderá solicitar à CGTI área de armazenamento em servidor de arquivo para se valer das garantias de continuidade e cópias de segurança (backup) dos mesmos;
- A autorização de acesso a uma pasta pública deverá ser feita pelo chefe da área solicitante. O pedido de alteração ou revogação de acesso também será feito nas mesmas condições.
- Os arquivos a serem armazenados nas pastas públicas serão os de natureza institucional. É vedado o armazenamento de arquivos não ligados às atividades profissionais ou os de natureza pessoal, respondendo à área responsável pela pasta pública pelo uso indevido da mesma.
- Caberá ao usuário periodicamente eliminar os arquivos que não tenham mais utilidade.

2.4. No uso da rede local são vedadas as seguintes ações:

- Qualquer tentativa de obter acesso não autorizado, de fraudar a autenticação de usuário ou segurança de servidores de rede ou contas de usuários. Isso inclui acesso aos dados não disponíveis para o usuário, tentativas de conectar-se a servidor ou conta de usuário cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de qualquer rede ou equipamento;
- Tentativa de interferir nos serviços de qualquer outro usuário, servidores ou da rede. Isso inclui ataques do tipo "negação de acesso", provocar congestionamento etc.;
- Utilizar a rede para tentar sobrecarregar ou invadir um servidor;
- Uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários;
- Utilização de material de natureza pornográfica e/ou racista, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;
- Criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas.

2.5. Sobre o acesso à rede local sem fio (wireless) do Ministério das Comunicações:

- O acesso à rede local sem fio se dará segundo o anexo II desta norma que é mantida por este Comitê. Ressalvados os casos excepcionais devidamente justificados.

3. REDE SEM FIO

3.1. Esta rede consiste em infraestrutura computacional de pontos de acesso de rede sem fio (*wireless Access Points* ou *wireless AP's*) e controlador de pontos de acesso, interligados à rede de dados interna cabeada do MC.

3.2. Descrição dos tipos:

- Visitante: Destinado a permitir aos visitantes do Ministério das Comunicações acesso à Internet para conveniência durante o período em que permanecerem nas instalações do MC. O acesso individual é atribuído através identificação de usuário e senha, realizada nas portarias de acesso às instalações do MC. Por motivo de segurança, esta rede não terá acesso à Intranet e demais serviços restritos aos usuários corporativos do Ministério das Comunicações.
- Produção: Destinado aos usuários corporativos do Ministério das Comunicações como alternativa ao acesso pela rede fixa cabeada convencional, sendo submetido às mesmas regras,

direitos e limitações que o seu perfil de acesso pela rede fixa cabeada lhe permite. O acesso individual é atribuído através identificação de usuário e senha, realizada a partir do cadastro no sistema corporativo do MC.

- Público: Destinado a permitir acesso aos visitantes do Ministério das Comunicações nos: espaços públicos, como salas de reuniões, auditório e recepções; ou em espaços destinados a autoridades, como gabinetes do Ministro e Secretários. O acesso é livre, sem identificação de usuário e senha, porém restrito fisicamente aos ambientes destinados ao público e autoridades. Por motivo de segurança, esta rede não terá acesso à Intranet e demais serviços restritos aos usuários corporativos do Ministério das Comunicações.

3.3. O acesso à rede PÚBLICO estará disponível somente em locais previamente determinados pelo Ministério, sem restrições de cadastramento e senha e somente para acesso à Internet através dos protocolos HTTP e HTTPS.

3.4. Como, por determinantes da própria tecnologia, não é possível restringir o sinal da rede sem fio aos limites estritos de uma área pequena, como um gabinete ou conjunto de salas contíguas, a disponibilização deste acesso, sem as restrições de cadastramento e senha, fará com que o sinal possa, eventualmente, ser captado e utilizado nas imediações das áreas pretendidas. Portanto, é possível que pessoas outras que não aquelas tidas como público-alvo venham, também, a usufruir deste acesso. Por esta razão, esta rede estará restrita a poucas áreas no Edifício Sede e Anexo do Ministério das Comunicações.

3.5. O acesso à rede PRODUÇÃO segue as regras e processos que norteiam o acesso à Intranet do Ministério das Comunicações. É necessário seguir os procedimentos padrão para obtenção de conta e senha de acesso, cadastramento nos sistemas de controle e configuração específica do equipamento computacional – portátil ou não – executada pelos técnicos da CGTI.

3.6. Apenas os dispositivos conectados à rede sem fio PRODUÇÃO terão acesso aos recursos internos (Intranet) do MC.

3.7. O acesso à rede VISITANTE dar-se-á através de cadastro de usuário e senha, obtidos na identificação dos visitantes nas portarias dos edifícios sede e anexo do Ministério das Comunicações. A rede VISITANTE é exclusiva para acesso à Internet por meio dos protocolos HTTP e HTTPS.

3.8. Entende-se por dispositivos móveis passíveis de cadastramento e autorização os computadores portáteis (*notebooks*, *netbooks*, *laptops*) e outros equipamentos (*tablets*, *smartphones*, *PDA*s e celulares) compatíveis com o padrão IEEE 802.11.

3.9. As redes VISITANTE e PÚBLICO não deverão ser utilizadas para trafegar informações sigilosas ou restritas do MC.

3.10. Todo tráfego da rede de dados sem fio será passível de monitoramento e investigação, caso haja indícios de quebra de segurança que comprometa a SIC no âmbito do MC.

3.11. O acesso a sítios impróprios ou que representam riscos à SIC estarão sujeitos a bloqueios automáticos realizados por filtro de conteúdo e de acordo com os procedimentos, normas e políticas de acesso vigentes no âmbito do MC.

3.12. Os privilégios de acesso de qualquer usuário, cujas atividades estejam em desconformidade com este documento ou demais normas e políticas de SIC vigentes no âmbito do MC, estarão sujeitos à suspensão temporária ou permanente ou sansões outras previstas nos instrumentos normativos do MC ou determinados pelo CGSIC do MC.

3.13. O tráfego de rede de dispositivo identificado como potencial ameaça à segurança da rede do Ministério das Comunicações estará sujeito ao bloqueio de sua conexão, até a devida averiguação dos

controles de segurança ou remoção das eventuais ameaças.

4. INTERNET

4.1. As normas de utilização da Internet englobam desde a navegação em sites até downloads e uploads de arquivos.

4.2. A CGTI reserva-se ao direito de bloquear ou liberar o acesso aos sítios de internet, desde que o ato esteja amparado por justificativa plausível.

4.3. Do uso da Internet/Intranet na rede local:

- É autorizado o acesso a endereços de internet de clientes, fornecedores, entidades acadêmicas, entre outros, naquilo que for pertinente ao trabalho realizado pelo usuário com objetivo de pesquisa e de aquisição de conhecimentos especializados;
- É autorizado o acesso a endereços externos de organizações bancárias e mercantis, em volume razoável, necessário ao atendimento de necessidades pessoais do usuário com o objetivo de proporcionar-lhe maior comodidade e agilidade;
- O usuário é responsável pelas informações e dados transmitidos ou recebidos por meio da Internet.

4.4. No uso de Internet/Intranet são vedadas as seguintes ações:

- Ações que possam resultar na invasão às estações de trabalho, microcomputadores, Internet/Intranet do Ministério das Comunicações ou de redes externas;
- Ações que possam resultar em acessos não autorizados a servidores da rede de Computadores do Ministério das Comunicações ou de redes externas;
- Cópia e distribuição de material ou software protegido por lei de direito autoral, por qualquer meio.

ANEXO IV

CORREIO ELETRÔNICO

1. OBJETIVO

Regulamentar os critérios e procedimentos para utilização dos serviços de correio eletrônico do MC.

2. UTILIZAÇÃO

2.1. Fica definido que a utilização de e-mail engloba desde o envio até o recebimento e gerenciamento das caixas de e-mail de usuários.

2.2. Da utilização do correio eletrônico:

- Todo servidor será o titular de uma única caixa postal no Correio Eletrônico do Ministério das Comunicações, salvo em casos de caixas corporativas com a devida autorização superior da CGTI;
- O titular da unidade administrativa detentora de Caixa Postal Corporativa do Correio Eletrônico do Ministério das Comunicações designará um responsável e um substituto pela administração da caixa, bem como os usuários que a ela terão acesso;

- O tamanho da caixa do Correio Eletrônico do usuário do Ministério das Comunicações para o envio e recebimento será determinado de acordo com o Anexo I desta Norma.

2.3. Os servidores deverão utilizar a assinatura padrão nos e-mails conforme definida pela Assessoria de Comunicação - ASCOM.

3. NA UTILIZAÇÃO DO CORREIO ELETRÔNICO SÃO VEDADAS AS SEGUINTES AÇÕES

3.1. Utilização de correio eletrônico distintos do provido pelo Ministério das Comunicações, inclusive os pessoais, para transmissão e recebimento de mensagens institucionais, exceto para os casos devidamente justificados;

3.2. Tentativa de acesso não autorizado à caixa postal de terceiros;

3.3. Tentativa de acesso não autorizado ao Servidor de e-mail;

3.4. Envio de informações sensíveis, classificadas ou proprietárias, inclusive senhas, para pessoas ou organizações, sem prévia e expressa autorização superior;

3.5. Envio intencional de material obsceno, ofensivo, ilegal ou antiético;

3.6. Envio de mensagens de e-mail ("junk mail" ou "spam") que, de acordo com a capacidade técnica da rede, seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade comercial ou não, anúncios, informativos e propaganda política;

3.7. Envio intencional de mensagens que contenham vírus ou qualquer forma de rotinas de programação de computador prejudiciais ou danosas;

3.8. Transmissão e/ou retransmissão de mensagens com finalidade comercial de interesse particular ou de terceiros;

3.9. Redirecionamento das caixas de Correio Eletrônico do Ministério das Comunicações, da qual o usuário é o titular, para correios de provedores externos. Exceto para os casos devidamente justificados;

3.10. Assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens;

3.11. Reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides";

3.12. Envio de e-mail mal-intencionado ou sobrecarregar um usuário, site ou servidor com e-mails muito extensos ou numerosos;

3.13. Utilizar e-mail como instrumento de ameaça, calúnia, injúria, difamação ou ofensa;

3.14. Envio de e-mail com arquivos anexos que comprometa o uso da rede ou perturbe o bom andamento dos trabalhos.

ANEXO V

SERVIÇOS DE TELEFONIA FIXA E MÓVEL

1. OBJETIVO

Regulamentar os procedimentos para os serviços de comunicação de voz por meio de telefonia fixa e móvel e de dados por meio dos dispositivos móveis do tipo tablet e modem com acesso à internet, no âmbito do Ministério das Comunicações.

2. DAS DISPOSIÇÕES GERAIS

2.1. Os serviços de comunicação de voz por meio de telefonia fixa e móvel e de dados por meio dos dispositivos do tipo celular, tablet e modem, com acesso à internet, destinam-se às necessidades de serviço.

2.2. O Ministério disponibilizará os equipamentos, aparelhos e acessórios para uso dos serviços conforme tabela de perfis citado no Anexo I desta Norma Operacional.

2.3. No ato do recebimento dos equipamentos, aparelhos e acessórios, os usuários deverão assinar o Termo de Responsabilidade.

2.4. O usuário não mais detentor de autorização para uso dos equipamentos, aparelhos e acessórios, deverá, necessariamente, devolver à CGTI para baixa do termo.

2.5. Será proibido ao usuário disponibilizar a linha/aparelho a outro servidor, sem autorização expressa da CGTI, o que, caso ocorra, acarretará no bloqueio imediato dos serviços.

2.6. Aos usuários ficará proibida a utilização dos serviços para o envio de telegramas, anúncios fonados, ligação para números 0900, 0300, disque amizade ou assemelhados, recebimento de ligações a cobrar e realização de chamadas telefônicas com o auxílio de telefonista.

2.7. Os custos decorrentes de eventual utilização indevida dos serviços deverão ser integralmente ressarcidos aos cofres da União, na forma prevista.

3. ATESTE E LIMITES DE UTILIZAÇÃO DOS SERVIÇOS

3.1. O controle das ligações realizadas será efetuado pelos gestores e/ou fiscais dos contratos, por meio dos relatórios fornecidos pelas empresas de telefonia fixa.

3.2. Os limites de valores para utilização dos serviços de comunicação de voz por meio de telefonia fixa, móvel e de dados estão definidos conforme tabela de perfis constantes no Anexo I desta Norma Operacional.

3.3. Excedidos os limites de consumo, constantes no Anexo I desta norma, caberá ao usuário o ateste individual da sua fatura no prazo máximo de 5 dias úteis após o recebimento.

3.4. Os valores que excederem os limites estabelecidos deverão ser recolhidos aos cofres da União, pelos respectivos usuários, mediante Guia de Recolhimento da União - GRU, no prazo máximo de cinco dias úteis, a contar do recebimento da fatura, ressalvados os casos de excepcionalidade.

3.5. Para efeito do cálculo dos limites estabelecidos, será computado o valor total da fatura emitida pela operadora prestadora dos serviços, excluídas as taxas fixas referentes à prestação do serviço.

3.6. O recolhimento dos valores excedentes ou decorrentes de ligações realizadas em caráter particular deverá ser feito mediante o preenchimento de formulário GRU disponível no Portal SIAFI, no endereço https://consulta.tesouro.fazenda.gov.br/gru/gru_simples.asp, com as seguintes informações obrigatórias:

I. Unidade Favorecida: 410003;

II. Gestão: 00001 - Tesouro Nacional;

III. Recolhimento: 18854-9 - Ressarcimento de ligações telefônicas; e

IV. CPF, nome do contribuinte/recolhedor, valor principal e valor total.

3.7. Em caso excepcional, e desde que devidamente justificado, o usuário poderá requerer a liberação do pagamento do valor excedente ao limite estabelecido para realização de despesas, por meio do formulário "Justificativa de Excedente do Consumo de Telefonia" no SEI, devidamente, assinado pelo usuário, pelo Coordenador-Geral imediato ou equivalente e aprovação da CGTI.

- No formulário, o servidor deverá relacionar todos os gastos constantes da fatura, com seus respectivos valores, inclusive as que estão dentro do limite estabelecido, ficando dispensado de listar aqueles que serão por ele ressarcidas.

3.8. O usuário ficará isento de ressarcir o montante relativo aos gastos a serviço, cuja justificativa tenha sido aprovada pela CGTI.

3.9. Caso a solicitação de excepcionalidade seja indeferida, o usuário deverá efetuar o recolhimento no prazo de cinco dias úteis, a contar da data de ciência do indeferimento.

4. DOS SERVIÇOS DE LONGA DISTÂNCIA NACIONAL E INTERNACIONAL

4.1. As ligações de longa distância nacional e internacional, nos serviços de comunicação de voz por meio de telefonia fixa e móvel, deverão ser realizadas, obrigatoriamente, por intermédio das operadoras contratadas pelo Ministério, devendo ser objeto de ressarcimento pelos usuários aquelas realizadas em desacordo com os serviços contratados.

4.2. Os serviços de voz e dados por meio de dispositivos móveis, para uso no exterior, ficam restritos conforme perfis definidos no Anexo I desta norma.

4.3. A solicitação de liberação temporária do serviço de comunicação de voz e dados para uso no exterior, deverá ser encaminhada a CGTI com no mínimo 2 dias úteis de antecedência a necessidade do serviço.

5. DAS RESPONSABILIDADES

5.1. Caberá ao usuário dos aparelhos, equipamentos e demais acessórios de comunicação cedidos pela empresa prestadora do serviço ou de propriedade do Ministério:

I. zelar pela guarda e conservação dos mesmos;

II. notificar imediatamente, por telefone a CGTI, os casos de perda, extravio de qualquer natureza, ou roubo, para que o serviço seja bloqueado e, posteriormente, por escrito, à CGTI, anexando a respectiva ocorrência policial;

III. comunicar imediatamente à operadora pelo número constante no termo de responsabilidade, quando os fatos previstos no inciso anterior ocorrerem fora do horário de expediente, nos finais de semana e feriados;

IV. repor o aparelho, equipamento e demais acessórios, sem ônus para o Ministério, ou o valor correspondente estipulado pela empresa contratada, nos casos de perda total dos mesmos, quer seja por dano, extravio, furto ou roubo, por meio de ressarcimento na forma prevista;

V. arcar com as despesas decorrentes do conserto do aparelho, equipamento e demais acessórios, nos casos em que constatado, pela empresa de assistência autorizada, defeito provocado por uso indevido;

VI. incluir e manter senha de bloqueio de acesso indevido; e

VII. devolver à CGTI o aparelho, equipamento e os acessórios descritos no Termo de Responsabilidade, em perfeitas condições de uso, inclusive no caso de alteração da situação funcional que justificou a concessão do serviço.

5.2. O usuário será responsável pelos danos causados aos aparelhos, equipamentos e demais acessórios de comunicação, em especial, quando constatada as seguintes ocorrências:

I. uso em desacordo com a finalidade e as aplicações para as quais foram projetados;

II. não observância no cumprimento das orientações contidas no Manual do Usuário ou em qualquer outra orientação de uso;

III. violação, modificação ou adulteração;

IV. ligação em instalação elétrica inadequada ou sujeita a flutuações excessivas ou diferentes das recomendadas no Manual do Usuário ou em qualquer outra orientação de uso;

V. acidentes, quedas, exposição à umidade excessiva ou à ação dos agentes da natureza, ou imersão em meios líquidos; e

VI. utilização com outros equipamentos ou acessórios que não os originais.

5.3. Será vedado aos usuários realizar qualquer alteração na estrutura ou nos programas instalados nos aparelhos, equipamentos e demais acessórios de comunicação.

5.4. À CGTI caberá configurar os dispositivos e instalar os programas homologados.

Documento assinado eletronicamente por **Ulysses Cesar Amaro de Melo**, **Subsecretário de Planejamento, Orçamento e Administração**, em 28/11/2014, às 15:31, conforme art. 3°, III, "a", da Portaria MC 89/2014.
N° de Série do Certificado: 6671162793238535884690770188957346642 4

A autenticidade do documento pode ser conferida no site http://sei.mc.gov.br/verifica.html informando o código verificador **0261908** e o código CRC **CE68B033**.

Criado por virginia.fidelis, versão 3 por virginia.fidelis em 28/11/2014 11:15:26.

Anexo F

Documentos enviados como anexo pelo Ministério da Ciência e Tecnologia

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO
SECRETARIA EXECUTIVA
SERVIÇO DE INFORMAÇÕES AO CIDADÃO
Esplanada dos Ministérios, Bloco E, Sala 133 – 70067-900 – Brasília - DF
Telefone: (61) 2033-8100

Brasília, DF, 13 de maio de 2015.

RESPOSTA AO PEDIDO DE INFORMAÇÕES Nº 01390.000508/2015-19

Prezado Senhor François Braga de Azevedo Filho,

Em atendimento ao Pedido de Informações nº 01390.000508/2015-19, postado no Sistema de Informações ao Cidadão, informamos a Vossa Senhoria que:

1 – Sim. O Ministério da Ciência, Tecnologia e Inovação possui política a respeito de e-mail corporativo;

2 – Sim. O uso do e-mail corporativo é obrigatório para os agentes públicos em atividade no MCTI, quando no exercício de suas funções; e

3 – Sim. Os e-mails corporativos de todos os servidores públicos e comissionados em atividade no MCTI são arquivados para futuras auditorias.

Atenciosamente,

Serviço de Informações ao Cidadão - SIC
Ministério da Ciência, Tecnologia e Inovação

Anexo G

Documentos enviados como anexo pelo Ministério das Relações Exteriores

Prezado Senhor Azevedo Filho,

Por meio da Portaria no. 43, de 26/01/2015, foi implementada a Política de Segurança da Informação e Comunicações (POSIC) do MRE, que estabelece os princípios para a utilização dos meios da tecnologia da informação e das comunicações por servidores do quadro permanente e contratados locais no exterior. A mesma POSIC criou o Comitê de Segurança da Informação e Comunicações (CSIC), presidido pelo Diretor do Departamento de Comunicações e Documentação (DCD) para: "assessorar as ações de segurança da informação e comunicações no âmbito do MRE; constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; propor normas e procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a legislação sobre o tema."
O referido Comitê manteve sua primeira reunião em março passado, com o objetivo de estabelecer, por instrumento normativo, as diretrizes para uso do correio eletrônico corporativo, para substituir a regulamentação anterior (Norma DCD 01/2006, abaixo transcrita**) .
A primeira versão da portaria foi amplamente debatida e deverá ser finalizada nas próximas semanas, com vistas a sua adoção e implementação ainda no correr do primeiro semestre. Uma vez que essa minuta constitui, nos termos da Lei de Acesso à Informação (Decreto no. 7.724/12, Artigo 20*), documento preparatório, ele só poderá ser divulgado quando da formalização da portaria. Tão logo publicada, portanto, cópia será encaminhada a Vossa Senhoria.
Assim como a POSIC, o cumprimento das futuras normas sobre utilização do correio eletrônico corporativo do domínio @itamaraty.gov.br será obrigatório para todos os servidores do quadro permanente e demais funcionários que mantém vínculo contratual com o Ministério das Relações Exteriores (empregados de empresas terceirizadas que prestam serviços ao MRE em Brasília e contratados locais dos postos no exterior).
O gerenciamento das caixas postais individuais ou coletivas é de responsabilidade exclusiva dos usuários, uma vez que ainda não há normal federal que regulamente a matéria. No entendimento da Comissão Mista de Reavaliação de Informações, todo o conteúdo de caixas postais de correios eletrônicos corporativos é de natureza pessoal, e assim protegido nos termos da lei. Apenas nos casos de suspeita de infração à Política de Segurança da Informação e Comunicações, a Divisão de Informática do MRE poderá acessar a caixa postal institucional do respectivo usuário através de ato administrativo ou judicial.

Atenciosamente,
Serviço de Informação ao Cidadão Ministério das Relações Exteriores

*Art. 20. O acesso a documento preparatório ou informação nele contida, utilizados como fundamento de tomada de decisão ou de ato administrativo, será assegurado a partir da edição do ato ou decisão.

**NORMA DCD nº1/2006

O DIRETOR DO DEPARTAMENTO DE COMUNICAÇÕES E DOCUMENTAÇÃO, no uso de suas atribuições, e em atendimento à Recomendação n° 01, de 9 de dezembro de 2002, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, DISPÕE sobre a utilização de correio eletrônico no Ministério das Relações Exteriores:

Art. 1º A presente norma tem como objetivo estabelecer regras para prestação e utilização dos serviços de correio eletrônico providos pelo Ministério das Relações Exteriores, visando a disciplinar a troca de mensagens eletrônicas e estabelecer critérios para que os mesmos sejam utilizados em conformidade com a legislação brasileira aplicável.

Art. 2º Esta norma aplica-se a todas as Unidades do Ministério das Relações Exteriores e usuários, servidores e prestadores de serviço, que utilizam o sistema de correio eletrônico disponível.

Art. 3º Os seguintes conceitos aplicam-se a essa normatização:

I. Considera-se serviço de correio eletrônico o sistema de mensagens utilizado para criar, enviar, encaminhar, responder, transmitir, arquivar, manter, copiar, mostrar, ler ou imprimir informações com o propósito de comunicação entre redes de computadores ou entre pessoas ou grupos;

II. Considera-se mensagem de correio eletrônico um ou mais registros eletrônicos de computador ou mensagens criadas, enviadas, encaminhadas, respondidas, transmitidas, arquivadas, mantidas, copiadas, mostradas, lidas ou impressas por um ou vários sistemas ou serviços de correio eletrônicos;

III. Considera-se usuário a pessoa física, seja servidor, empregado ou prestador de serviços; a unidade administrativa ou grupo de trabalho com reconhecimento e habilitação pela administração ao uso do serviço de correio eletrônico;

IV. Considera-se identificação do usuário ou nome do usuário a forma com que este é reconhecido pelo ambiente de informática do Ministério das Relações Exteriores, ao qual se acede mediante "login" e senha e que permite a utilização de ações e ferramentas de acordo com o perfil delimitado;

V. Considera-se caixa postal a área de armazenamento que contém todas as pastas do correio eletrônico, dentre as quais a caixa de entrada - área predefinida que armazena mensagens recebidas; e a caixa de saída - área predefinida que armazena as mensagens enviadas, até que sejam entregues ao destinatário;

VI. Considera-se lista de discussão o grupo de usuários de correio eletrônico criado com objetivo de trocar informações relacionadas a uma determinada área ou assunto; e

VII. Considera-se pasta pública a área destinada a armazenar informações direcionadas a um determinado assunto, tratado por um grupo definido pelo administrador da rede sob solicitação de algum usuário.

Da Utilização do Correio Eletrônico

Art. 4º O serviço de correio eletrônico visa à troca de mensagens com assuntos pertinentes às atividades do Órgão.

Art. 5º O serviço de correio eletrônico deve ser extensivamente utilizado no desempenho das atividades funcionais, com vistas à racionalização do trabalho e ao aumento da produtividade por meio da facilitação da troca de informações e do intercâmbio de idéias.

Art. 6º O acesso ao correio eletrônico dá-se pelo conjunto identificação do usuário (login), caixa postal e senha, que é pessoal e intransferível.

Art. 7°-. O reconhecimento e a habilitação do uso do serviço de correio eletrônico para unidades administrativas, grupos de trabalho e outros usuários despersonalizados ficará a cargo da administração do serviço, no caso a Chefia da Divisão de Informática (DINFOR).

Par. 1° - Somente será considerada a possibilidade de atribuição de privilégios a usuário despersonalizado quando a Unidade comprovar a necessidade dessa exceção.

Par. 2° - Quando do reconhecimento e habilitação de uso do serviço de correio eletrônico para unidades administrativas, grupos de trabalho e outros usuários despersonalizados, deverá ser identificada junto ao administrador do serviço a pessoa responsável pelo uso do correio destes usuários.

Art. 8º É vedada tentativa de acesso não autorizado às caixas postais de terceiros.

Art. 9º Prestadores de serviços terceirizados e estagiários poderão, durante o período de prestação dos serviços, a critério do responsável pela área onde está sendo prestado o serviço terceirizado ou estágio e no interesse do serviço, ter acesso ao correio eletrônico institucional, observando as normas aqui enumeradas.

Art.10º O remetente deve-se identificar de forma clara e evidente em todas as suas comunicações eletrônicas, não sendo permitidas alterações ou manipulações da origem das postagens.

Parágrafo único. As mensagens deverão ser redigidas de forma clara e sucinta, devendo conter o grau de formalidade compatível com o destinatário e o assunto tratado.

Art. 11° Aplicam-se ao correio eletrônico as normas de classificação de informações vigentes na Administração Pública Federal, conforme legislação em vigor.

Art. 12° É vedado o envio e o armazenamento de mensagens contendo:

I - material obsceno, ilegal ou antiético;

II - anúncios publicitários;

III - listas de endereços eletrônicos dos usuários do Correio Eletrônico do Órgão;

IV - vírus ou qualquer outro tipo de programa danoso;

V - material protegido por leis de propriedade intelectual;

VI - entretenimentos e "correntes";

VII -material preconceituoso ou discriminatório;

VIII - material de natureza político-partidária ou sindical, que promova a eleição de candidatos para cargos públicos eletivos, clubes, associações e sindicatos;

IX - assuntos ofensivos;

X - músicas, vídeos ou animações que não sejam de interesse específico do trabalho; e

XI - programas de computador.

Art. 13. É permitida, ao usuário, a participação em listas de discussão com assuntos relacionados exclusivamente ao interesse do trabalho, tanto profissionais quanto educativos.

Art. 14. É permitido, ao usuário, o envio de mensagens para até 15 destinatários, internos ou externos.

Parágrafo único. Os demais usuários que, no interesse do trabalho, necessitarem enviar mensagens com número maior de destinatários devem solicitar essa facilidade justificando sua necessidade à Divisão de Informática, que avaliará devidamente o pedido.

Das Competências

Art. 15. A Divisão de Informática é responsável pela administração do serviço de correio eletrônico do Ministério das Relações Exteriores.

Art. 16. A administração do correio eletrônico mantém ferramenta para atualização de dados cadastrais dos usuários. Os dados informados são de responsabilidade da Divisão de Pessoal (DP) e do próprio usuário.

Art. 17. A administração do correio eletrônico poderá, no caso de mudança de endereço eletrônico, quando solicitado pela chefia imediata ou superior, possibilitar o redirecionamento de mensagens a ele destinadas, desde que pertencente ao diretório da Rede Governo, por um prazo máximo de 30 dias.

Art. 18. Compete ao usuário:

I - gerenciar compromissos, contatos, tarefas, arquivos e atividades;

II - utilizar o correio eletrônico institucional para os objetivos e funções próprios e inerentes às suas atribuições funcionais;

III - eliminar periodicamente as mensagens contidas nas caixas postais;

IV - não permitir acesso de terceiros ao correio eletrônico por meio de sua senha; e

V - atualizar seus dados cadastrais utilizando os meios disponíveis.

Art. 19. Compete à administração do serviço de correio eletrônico:

I - garantir a disponibilidade do serviço de correio eletrônico em níveis de serviço adequados à necessidade do trabalho;

II - garantir a recuperação de mensagens em caso de danos ao ambiente, observando o prazo especificado no Art. 16o.;

III - criar caixas virtuais coletivas (CVC), oferecendo opções para os usuários destas, de inclusão e exclusão de usuários com permissões de uso escolhidas por ele;

IV - prever a possibilidade de criação de usuário despersonalizado, nos termos do Artigo 7°, quando houver comprovada necessidade de serviço.

V - criar pastas públicas para armazenar e divulgar documentos em discussão por um grupo determinado, oferecendo opções para os usuários destas, de inclusão e exclusão de usuários com permissões de uso escolhidas por ele;

VI - criar Listas de Discussão;

VII - desenvolver ações que garantam a operacionalização desta norma; e

VIII - divulgar esta norma aos usuários.

Art. 20. Para poder utilizar o serviço de correio eletrônico institucional, o usuário deve tomar conhecimento, por meio eletrônico ou impresso, de termo de responsabilidade, tomando ciência e concordando com os termos desta norma.

Art. 21. Os usuários deverão notificar a administração do correio eletrônico e sua chefia imediata ou superior, quando do recebimento de mensagens que contrariem o disposto nesta norma.

Da Apuração de Responsabilidades

Art. 22. Havendo indícios de que mensagens veiculadas pelo correio eletrônico possam ocasionar quebra de segurança ou violação de quaisquer das vedações constantes deste ou outro ato normativo, a administração do correio eletrônico adotará, imediatamente, medidas para a sua apuração, utilizando-se, para tanto, dos meios e procedimentos legalmente previstos.

Art. 23. Caracterizado o descumprimento de qualquer dos itens desta norma, caberá à administração do correio eletrônico informar a chefia imediata ou superior do usuário, apresentando o ocorrido a fim de encaminhar as providências de apuração de responsabilidades.

Das Disposições Gerais

Art. 24. As solicitações de novas caixas postais deverão ser encaminhadas à Central de Atendimento (CAT), pela chefia imediata ou superior com os respectivos dados cadastrais.

Parágrafo único.- Aos servidores aposentados poderá ser facultada a utilização de correio eletrônico, a critério da Administração.

Art. 26. Cabe à Divisão de Pessoal informar à Divisão de Informática as ocorrências decorrentes de afastamentos superiores a três meses de servidores.

Parágrafo único - No caso de afastamento definitivo, a Administração do correio eletrônico providenciará a exclusão da caixa postal.

Art. 27. Cabe a cada unidade administrativa comunicar à Divisão de Informática o desligamento de empregados terceirizados, temporários e estagiários sob sua responsabilidade para a exclusão definitiva da caixa postal.

Art. 28. A caixa postal sem movimentação por um período igual ou superior a três meses será bloqueada automaticamente pela administração do correio eletrônico.

Art. 29. Caberá à Divisão de Informática decidir sobre os casos omissos nesta norma.

HÉLIO VITOR RAMOS FILHO

*Art. 20. O acesso a documento preparatório ou informação nele contida, utilizados como fundamento de tomada de decisão ou de ato administrativo, será assegurado a partir da edição do ato ou decisão.

Publicada no Boletim de Serviço nº 121, de 29/06/2015

Ato do Gestor de Segurança da Informação e Comunicações

PORTARIA CSIC Nº 1, DE 19 DE JUNHO DE 2015

Estabelece as normas para uso do correio eletrônico corporativo.

1. ABRANGÊNCIA E CAMPO DE APLICAÇÃO:

1.1. Esta norma dispõe sobre as regras de segurança para uso do correio eletrônico corporativo do Ministério das Relações Exteriores (MRE), @itamaraty.gov.br, que devem ser observadas em todas as suas unidades na Secretaria de Estado das Relações Exteriores (SERE), nos Escritórios Regionais e nos Postos no Exterior.

2. DEFINIÇÕES E TERMINOLOGIAS

2.1. Caixa postal: conjunto de elementos necessários para o funcionamento do correio eletrônico, tais como pastas (caixa de entrada, itens enviados, rascunhos, etc.) e as próprias mensagens.

2.2. Cavalo de Tróia: programa, normalmente recebido como presente (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc.), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

2.3. Conta de correio eletrônico: identificação do proprietário de uma caixa postal.

2.4. Correio eletrônico institucional: conta de correio eletrônico provido pelo MRE precipuamente para servidor do Quadro Permanente do MRE e para outros funcionários nos termos desta Portaria, no domínio @itamaraty.gov.br.

2.5. Correio eletrônico particular: conta de correio eletrônico mantido por terceiros (Gmail, Hotmail, Yahoo, etc.).

2.6. Corrente: é uma forma de "spam" caracterizada pelo envio de uma mensagem que pede ao destinatário que a repasse a outros usuários ou para todos aqueles em sua lista de endereços.

2.7. Servidor do Quadro Permanente do MRE: é o servidor das carreiras que integram o Serviço Exterior Brasileiro, ou servidor do PGPE e PCC.

2.8. Lista de discussão: ferramenta que permite a troca controlada de mensagens entre os membros de um grupo.

2.9. Lista de distribuição: uso de um endereço definido pelo usuário para o envio de mensagens (unidirecional) aos membros de um grupo; ao contrário da lista de discussão, não permite o envio de mensagens entre os membros do grupo.

2.10. Provedor de correio externo: fornecedor privado de serviços de correio eletrônico (Gmail, Yahoo, Hotmail, etc.).

2.11. "Spam": termo que designa mensagens de correio não solicitadas, geralmente enviadas para grande número de destinatários.

2.12. "Spyware": categoria de programas que monitoram, geralmente sem autorização e maliciosamente, as atividades de sistemas e enviam as informações coletadas para terceiros.

2.13. Unidades descentralizadas: são os Escritórios Regionais e as duas Comissões Demarcadoras de Limites.

2.14. Usuário: todo aquele que possui acesso autorizado aos ativos de tecnologia da informação do MRE.

2.15. Vírus: programa malicioso que se propaga infectando a outros sistemas e equipamentos, por meio da distribuição de cópias de si mesmo.

3. DOS PROGRAMAS DE CORREIO ELETRÔNICO:

3.1. Cabe à Divisão de Informática (DINFOR) definir os programas homologados para o correio eletrônico institucional do MRE.

3.2. É atribuição do Gestor de Segurança da Informação normatizar o uso do correio eletrônico particular em equipamentos da rede do MRE.

3.3. É proibido o uso de provedores de e-mail externos para o encaminhamento das mensagens de uma caixa postal do MRE.

4. DA CONCESSÃO DE ACESSO AO CORREIO ELETRÔNICO E CONTA DE USUÁRIO:

4.1. Somente será concedido endereço de correio eletrônico corporativo a usuário que tenha vínculo estatutário ou contratual com o MRE, ou que seja empregado local dos postos no exterior, de acordo com as regras seguintes.

4.2. A solicitação de abertura de caixa de correio deve ser encaminhada à Central de Atendimento Técnico – CAT:

4.2.1. Pelo Chefe imediato do usuário na SERE utilizando o Formulário Eletrônico de Cadastro na Rede da SERE, disponível no verbete correspondente na Diplopédia; ou

4.2.2. No caso de usuário lotado em posto no exterior ou unidade descentralizada, por telegrama distribuído a CAT/DINFOR, que informe o nome completo do usuário, sua categoria funcional, e a razão de serviço que justifique a concessão de caixa de correio institucional.

4.3. A partir de 1º de novembro de 2015, adidos de outros órgãos públicos e colaboradores eventuais deverão utilizar exclusivamente os endereços institucionais de seus órgãos ou empresas de origem.

4.4. O usuário terá direito a uma única conta de e-mail que o identificará univocamente em todo MRE.

4.5. A estagiários do CIEE nas unidades da SERE, mediante justificada razão de serviço, poderá ser concedido acesso a caixa de correio interna, exclusivamente para comunicações dentro da rede do MRE, seguindo o procedimento descrito em 4.2.1.

4.6. Nos casos em que seja necessário expedir mensagem de correio preparada por estagiário para fora da rede do MRE, caberá ao chefe da unidade fazê-lo.

4.7. A funcionários de empresas terceirizadas que prestem serviço continuado à SERE, mediante justificada razão de serviço, poderá ser concedido acesso a caixa de correio interna, exclusivamente para comunicações dentro da rede do MRE, seguindo o procedimento descrito em 4.2.1.

4.8.Estagiários e funcionários de empresas terceirizadas que prestem serviços a postos no exterior devem utilizar suas caixas de e-mail privadas, sendo-lhes vedado o acesso a caixa de correio institucional.

5. ENCERRAMENTO DE CONTAS DE USUÁRIO E DE CORREIO ELETRÔNICO:

5.1. No momento da aposentadoria de servidores do Quadro Permanente do MRE, a Divisão do Pessoal cadastrará endereço de correio particular para cada servidor aposentado, informando-o de que a conta corporativa será desativada no período de até 60 dias, a contar da data de entrada do pedido de aposentadoria.

5.1.1. Os servidores que, na data de publicação desta portaria, já estejam aposentados, deverão informar o seu endereço de correio particular à Divisão de Pagamentos por ocasião do recadastramento anual.

5.2. É responsabilidade do Chefe do Posto no exterior, incluir a distribuição CAT no expediente dirigido à SERE/SCL em que é comunicado o encerramento de relação contratual com empregado local (auxiliar técnico, auxiliar administrativo, assistente técnico, auxiliar de apoio, diretor de Centro Cultural, etc.), e solicitar a desativação da conta de correio correspondente.

5.3. É responsabilidade do Chefe de unidade descentralizada comunicar à SERE, por telegrama com distribuição CAT, o encerramento de relação contratual com estagiários que porventura possuam conta de correio eletrônico, e solicitar a desativação da conta de correio correspondente.

5.4.É responsabilidade do Chefe da DTA comunicar à CAT, por mini-memo, o encerramento das atividades de estagiários na SERE que porventura possuam conta de correio eletrônico, e solicitar a desativação da conta de correio correspondente.

6. BLOQUEIO OU DESBLOQUEIO DO CORREIO ELETRÔNICO:

6.1. Cabe à Divisão do Pessoal solicitar à Central de Atendimento (CAT) o bloqueio ou desbloqueio da conta de correio do usuário do Quadro Permanente do MRE, de acordo com a situação funcional do servidor.

6.2. Cabe à SCL/DAEX solicitar à Central de Atendimento (CAT) o cancelamento, bloqueio, ou desbloqueio da conta de correio de usuário que seja contratado local (assistente técnico, auxiliar técnico, auxiliar administrativo, auxiliar de apoio, etc.).

6.3.Cabe à DPLP solicitar à Central de Atendimento (CAT) o cancelamento, bloqueio, ou desbloqueio da conta de correio de usuário que seja contratado por suas dotações (diretor de Centro Cultural, etc.).

6.4. As contas de correio institucional que permanecerem inativas por período de seis meses, serão automaticamente suspensas e sua reativação dependerá de solicitação do usuário à CAT.

7. DAS CAIXAS POSTAIS CORPORATIVAS:

7.1. Para efeitos desta Portaria, chama-se "caixa postal corporativa" a caixa de correio que leva o nome de uma unidade administrativa ou de um setor de posto no exterior ou unidade descentralizada.

7.2. Por questões de segurança e integridade do serviço de correio, é vedada a criação de caixa postal corporativa que não tenha um titular identificado dentre os servidores do Quadro Permanente do MRE.

7.3.O titular da caixa postal corporativa de uma unidade ou setor é o respectivo chefe.

7.4. O titular da caixa postal corporativa é responsável por:

7.4.1. Distribuir as mensagens eletrônicas recebidas, da mesma forma que o chefe de uma unidade distribui os expedientes de papel a ela destinados;

7.4.2. Providenciar que seu substituto legal tenha acesso à caixa corporativa em seus impedimentos;

7.4.3. Zelar pela segurança da senha associada à caixa corporativa; e

7.4.4. Utilizar as funcionalidades de regras automáticas do programa de correio para fortalecer a gestão de expedientes eletrônicos em sua unidade.

7.5. As caixas postais corporativas devem ser utilizadas somente com a finalidade de receber e enviar mensagens em nome de uma unidade administrativa ou setor.

7.6. Para envio automático de uma mensagem a uma série de destinatários previamente definidos deve ser utilizada lista de distribuição, a ser configurada pelo próprio usuário.

8. DA RESPONSABILIDADE NA UTILIZAÇÃO DO CORREIO ELETRÔNICO:

8.1. O correio eletrônico institucional é o meio eletrônico exclusivo para comunicação de assuntos institucionais de caráter ostensivo, tanto internamente no MRE quanto com seus interlocutores externos.

8.1.1. A Corregedoria do Serviço Exterior (COR) poderá utilizar o correio eletrônico institucional para comunicação de arquivos criptografados que contenham assuntos de caráter sigiloso relativos, exclusivamente, a procedimentos disciplinares em curso (investigação preliminar, Sindicância Investigativa, Sindicância Punitiva e Processo Administrativo Disciplinar), tanto internamente no MRE quanto com seus interlocutores externos.

8.2. A conta de correio eletrônico institucional é pessoal e intransferível, e seu titular é o único responsável por seu uso.

8.3. O usuário de correio eletrônico deverá observar os princípios da ética, do bom senso e da razoabilidade do conteúdo trafegado e levar em devida conta seus eventuais riscos para a instituição.

8.4. O usuário deverá alterar periodicamente as senhas pessoais do correio eletrônico institucional.

8.5. As caixas postais do correio eletrônico institucional possuem tamanho limitado, que será fixado pela DINFOR, conforme a capacidade e disponibilidade de área de armazenamento; caso seja necessário manter mensagens de trabalho que ultrapassem o limite de armazenamento da caixa postal, o usuário deverá transferir as mensagens para arquivo local no programa de correio institucional, conforme instruções disponíveis na Diplopédia/Intratec.

8.6. É obrigação do usuário eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive nas pastas personalizadas, e nas pastas "lixeira", "rascunho" e "enviados", de forma a não exceder o limite de tamanho da caixa postal.

8.7. Uma vez ao ano será realizada limpeza automática de todas as mensagens com data superior a um ano, precedida por alertas aos usuários expedida pela CAT.

8.8. Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar o limite de tamanho estabelecido pela DINFOR.

8.9. É vedado o uso de correio particular para trato de assuntos institucionais, exceto em situações emergenciais que o justifiquem.

8.10. É vedada a utilização do correio eletrônico institucional para:

8.10.1. Fins particulares;

8.10.2. Trato de assuntos sigilosos, à exceção do previsto no item 8.1.1.;

8.10.3. Realizar distribuição de mensagens não solicitadas, sem caráter institucional, a grande número de destinatários ("spam");

8.10.4. Participar de correntes de mensagens eletrônicas;

8.10.5. Fins estranhos à missão do MRE;

8.10.6. Receber de forma consentida, armazenar ou enviar mensagens com:

8.10.6.1. Vírus de computador (cavalo de Tróia, "spyware", "malware", e outros códigos maliciosos);

8.10.6.2. Material pornográfico ou ofensivo à moral e aos bons costumes;

8.10.6.3. Conteúdo ilegal ou que faça apologia a crime;

8.10.6.4. Conteúdo discriminatório (racial, religioso, etc.) ou de incitação à violência;

8.10.6.5. Conteúdo que viole direitos autorais.

8.11. De forma a colaborar para o bom funcionamento do serviço de correio eletrônico institucional, o usuário deve EVITAR:

8.11.1. Abrir mensagens de origem desconhecida ou mesmo de usuários da rede @itamaraty.gov.br que contenham anexos suspeitos;

8.11.2. O reencaminhamento a outros usuários de mensagens de origem desconhecida ou que contenham anexos suspeitos; essas devem ser enviadas exclusivamente à caixa spam@itamaraty.gov.br;

8.11.3. Clicar em "links" de acesso a páginas de Internet em mensagens de correio recebidas de origem desconhecida, que podem iniciar a instalação de "softwares" maliciosos, direcionar o usuário para um sítio falso, capturar informações, senhas, etc.;

8.11.4. Abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico sem antes verificar sua procedência; no caso de suspeita de irregularidade na mensagem, o usuário deve solicitar ajuda à CAT.

8.11.5. Inserir senha de acesso à rede da SERE ou do posto em mensagem de correio.

8.11.6. O envio de mensagens com "links" para inserção de senhas, instruções de atualização ou pedidos de informações pessoais.

8.12. O MRE não é responsável por prover suporte técnico a contas de correio eletrônico particular.

9. BOAS PRÁTICAS:

9.1. São consideradas boas práticas de uso do correio eletrônico institucional e devem ser observadas por todos os usuários da rede MRE as seguintes:

9.1.1. Documentos digitalizados devem ser salvos em pastas individuais e/ou coletivas, na rede da SERE ou na rede interna do posto, conforme a localização da unidade, evitando-se a opção de envio desses documentos por correio eletrônico.

9.1.2. Os usuários devem sempre verificar a procedência das mensagens recebidas em suas caixas e eliminar e bloquear no "lixo eletrônico" mensagens suspeitas e, se for o caso, enviá-las para o endereço spam@itamaraty.gov.br.

9.1.3. Instruções e normas sobre gestão de contas e senhas jamais serão transmitidas por correio eletrônico.

9.1.4. Usuários que acessem o correio eletrônico institucional ou a Intratec a partir de computadores pessoais domésticos ou em viagens devem dispor de antivírus, anti-"spyware" e "firewalls" ativos em seus equipamentos, bem como de sistema operacional atualizado.

9.1.5. Caso não seja possível manter nível de segurança comparável ao que protege os computadores da SERE ou dos postos, recomenda-se a não utilização dos sistemas e correio eletrônico institucionais em computadores pessoais.

9.1.6. Recomenda-se a preferência por acesso remoto ao correio eletrônico (fora do ambiente da rede da SERE ou do Posto) por meio de telefone celular ou tablete.

9.1.7. Para os postos com setores que necessitem enviar mensagens de correio a mais de 100 destinatários, devem ser examinadas formas alternativas de difundir as informações, como a divulgação dessas por meio do sítio da internet, mídias sociais do Posto ou mecanismos de assinatura.

9.1.8. Caso seja imperioso o envio de mensagens por correio eletrônico a um grande grupo de destinatários, esses devem ser divididos em várias mensagens, que individualmente não excedam 100 destinatários, de forma a evitar que endereço corporativo do MRE seja incluído em listas de "spam".

10. MONITORAMENTO:

10.1. A fim de assegurar a observância das normas para uso do correio eletrônico institucional, todas as contas podem ser monitoradas e limitadas pela Divisão de Informática quanto à origem, destino, quantidade, conteúdo, anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados).

10.2. Nos casos de suspeita de infração à Política de Segurança da Informação e Comunicações, a DINFOR poderá acessar a caixa postal institucional do respectivo usuário com base em ato administrativo formal, como memorando com despacho do Subsecretário-Geral do Serviço Exterior, ou em cumprimento a ordem judicial.

11. DISPOSIÇÕES FINAIS

11.1. Os usuários devem comunicar prontamente à CAT incidentes que afetem a segurança dos ativos ou o descumprimento desta norma.

11.2. Em casos de quebra de segurança da informação por meio de recursos de TI, a CAT deve ser imediatamente comunicada.

11.3. Ao autor de infração a esta norma, serão aplicadas as sanções cabíveis conforme previsto no capítulo “Penalidades” da Política de Segurança da Informação e Comunicações do MRE.

12. VIGÊNCIA E ATUALIZAÇÃO

12.1. Esta Portaria entra em vigor a partir da data de sua publicação e sua atualização ocorrerá sempre que se fizer necessário.

12.2. Fica revogada a Portaria DCD 1/2006, publicada no Boletim de Serviço nº 202, de 20/10/2006.

JOÃO PEDRO CORRÊA COSTA