REVOGADO

PORTARIA Nº 500, DE 26 DE NOVEMBRO DE 2012. O SUBSECRETÁRIO DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO, DA SECRETARIA-EXECUTIVA DO MINISTÉRIO DAS COMUNICAÇÕES, no uso de suas atribuições e da competência que lhe foi atribuída no art. 72, capítulo V, do Anexo II, do Regimento Interno, aprovado pela Portaria nº 143, de 9 de março de 2012, publicada no D.O.U. de 12 seguinte, resolve:

Art. 1º Instituir a **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO MINISTÉRIO DAS COMUNICAÇÕES – POSIC,** em anexo.

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

ULYSSES CESAR AMARO DE MELO – Subsecretário de Planejamento, Orçamento e Administração

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DO MINISTÉRIO DAS COMUNICAÇÕES - POSIC

REFERÊNCIAS NORMATIVAS

Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Contém as emendas constitucionais posteriores. Brasília, DF: Senado, 1988.

Lei nº 7.232, de 29 de Outubro de 1984, que dispõe sobre a política nacional de Informática, e dá outras providências.

Lei nº 8.027, de 12 de Abril de 1990, que dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências.

Lei nº 8.112, de 11 de Dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

Lei nº 8.159, de 08 de Janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

Lei nº 8.429, de 02 de junho de 1992, que dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências.

Lei nº 9.983, de 14 de Julho de 2000, altera o decreto Lei nº 2.848/40 – Código Penal – tipificação de crimes por computador contra a Previdência Social e Administração Pública.

Decreto nº 1.048, de 21 de Janeiro de 1994, que dispõe sobre o Sistema de Administração dos Recursos de Informação e Informática, da Administração Pública Federal, e dá outras providências.

Decreto nº 1.171, de 24 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do poder executivo Federal, e outras providências.

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

Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados e informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado;

Decreto nº 6.029, de 01 de Fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências.

ABNT NBR ISO 27002:2005 – Código de Práticas para a Gestão da Segurança da Informação.

Acórdão 1603/2008 do Plenário do Tribunal de Contas da união – TCU

Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

Norma Complementar nº 02 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 13 de outubro de 2008, que define uma metodologia de Gestão de Segurança da Informação e Comunicações;

Norma Complementar nº 03 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 03 de julho de 2009, que define diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

Norma Complementar nº 04 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 14 de agosto de 2009, que define as diretrizes para o processo de gestão de riscos e segurança da informação.

Norma Complementar nº 05 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 14 de agosto de 2009, que define diretrizes para disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 06 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 11 de novembro de 2009, que define as diretrizes para o processo de gestão de continuidade de negócios.

Norma Complementar nº 07 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 06 de maio de 2010, que estabelece as diretrizes para implementação de controle de acesso relativo à segurança da informação e comunicação nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 08 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 19 de agosto de 2010, que estabelece as diretrizes para gerenciamento de incidentes de redes computacionais nos órgãos e entidades da Administração Pública Federal.

Norma Complementar nº 09 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 19 de novembro de 2010, que estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em segurança da informação e comunicação nos órgãos e entidades da Administração Pública Federal direta e indireta.

CAMPO DE APLICAÇÃO

Esta Política se aplica no âmbito do Ministério das Comunicações.

SUMÁRIO

1. OBJETIVO

Orientar as ações de segurança com o intuito de incorporar à estrutura de comunicação e informação do Ministério das Comunicações, na maior extensão possível, as características de integridade, privacidade, autenticidade, não repúdio e disponibilidade.

2. TERMOS E DEFINIÇÕES

Para entendimento da POSIC considera-se:

2.1 Segurança da Informação e Comunicação: ações que objetivam incorporar na estrutura de sistemas de informação e comunicação as características de confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio;

a) Confidencialidade: somente as pessoas devidamente autorizadas pela organização devem ter acesso à informação.

b) Integridade: somente as operações de alteração, supressão e adição autorizadas pela organização devem ser realizadas nas informações.

c) Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário e solicitado.

d) Autenticidade: princípio de segurança que assegura ser do autor a responsabilidade pela criação ou divulgação de uma dada informação.

e) Não-Repúdio: garantia que o emissor de uma mensagem ou executor de uma ação posteriormente não irá negar a autoria da mensagem ou ação, permitindo a sua identificação.

2.2 Política de Segurança da Informação e Comunicação: conjunto de diretrizes, normas, critérios e orientações estabelecidas pelo Ministério das Comunicações visando a implantação da segurança da informação e comunicação;

2.3 Comitê Gestor de Segurança da Informação e Comunicações: grupo de pessoas responsáveis por tratar os assuntos relativos à segurança da informação e comunicações no âmbito do Ministério das Comunicações;

2.4 Equipe de Tratamento e Resposta à Incidentes de Segurança: grupo de pessoas com a responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de Segurança no âmbito da estrutura de TIC do Ministério das Comunicações;

2.5 Incidente de Segurança:

i) ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

ii) é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas computacionais ou redes de comunicação.

3. PRINCÍPIOS

As ações relacionadas com à Segurança da Informação e Comunicação no MC são norteadas pelos seguintes princípios:

3.1 Responsabilidade: todos os colaboradores do Ministério das Comunicações são responsáveis pelo tratamento da informação e pelo cumprimento das normas de segurança da informação e comunicação;

3.1.1 Colaboradores: São os servidores, prestadores de serviço, mão-de-obra terceirizada, consultores, estagiários e qualquer outra pessoa que possua vínculo direto ou indireto com o MC ou que se utilize dos recursos de TI deste Ministério.

3.2 Conhecimento: todos os colaboradores do Ministério das Comunicações tomarão ciência das normas de segurança da informação e comunicação para o pleno desempenho de suas atribuições;

3.3 Legalidade: as ações de segurança da informação e comunicação levarão em consideração as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do Ministério das Comunicações formalmente estabelecidas;

3.4 Proporcionalidade: o nível, a complexidade e os custos das ações de segurança da informação e comunicação no MC serão adequados à criticidade, ao risco e ao valor do ativo a proteger.

3.5 Pró-Atividade: os colaboradores do Ministério das Comunicações devem comunicar imediatamente qualquer descumprimento ou violação desta Política e/ou das suas Normas e Procedimentos.

4. DIRETRIZES GERAIS

Os colaboradores do Ministério das Comunicações devem observar que:

4.1 A informação é um patrimônio do Ministério das Comunicações, órgão responsável pela sua produção. O seu acesso a estas informações não garante direito sobre as mesmas, mas sim a responsabilidade de protegê-las, assim como não confere autoridade para distribuí-las ou para liberar o acesso a outros;

4.2 O acesso à informação deve ser regulamentado por normas específicas de tratamento da informação;

4.3 As ações para garantir confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio devem considerar os critérios relativos à gestão de riscos e à gestão de continuidade dos negócios;

4.4 O recebimento e a instalação de recursos computacionais, tais como os programas aplicativos e sistemas homologados, somente podem ser realizados por pessoal credenciado do setor responsável pela Tecnologia da Informação; é vedado a utilização de programas aplicativos (*softwares*) e sistemas não homologados;

4.5 A aquisição e/ou contratação de bens ou serviços relativos a recursos de TI pressupõe estudo e análise prévios por parte do setor responsável pela Tecnologia da Informação;

4.6 A aquisição e/ou contratação de bens ou serviços relativos a recursos de TI pressupõe a inclusão de cláusulas de segurança e de trilhas de auditoria em seus contratos, quando aplicável;

4.7 As credenciais de acesso ("login" e senha) são pessoais e intransferíveis;

4.8 Cada área de atuação do MC poderá instituir suas normas de segurança levando em consideração as diretrizes desta POSIC e a legislação vigente, não podendo, entretanto, ser contrárias às normas vigentes neste Ministério.

5. RESPONSABILIDADES

5.1 O Comitê Gestor de Segurança da Informação e Comunicações (CGSIC) será integrado por representantes da estrutura organizacional do Ministério das Comunicações, podendo ser convidados, de acordo com a necessidade, consultores, fornecedores e responsáveis por áreas específicas que porventura não façam parte do Comitê, para fins de assessoramento técnico e sem direito a voto.

5.2 Ao Comitê Gestor de Segurança da informação e Comunicações (CGSIC), sem prejuízo das atribuições previstas na sua portaria de criação, compete:

I – Promover a implantação das ações e da cultura de segurança da informação e comunicação;

II - Constituir grupos de trabalho para tratar temas oportunos e propor soluções específicas sobre segurança da informação e comunicação;

III - Definir Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com a legislação vigente.

IV - Definir Normas e Procedimentos internos relativos à classificação das informações e procedimentos de tratamento, incluindo o uso de recursos de criptográficos.

V - Acompanhar as investigações e as avaliações dos danos decorrentes de eventuais incidentes ou quebras de segurança;

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

VII - Realizar e acompanhar estudos de novos instrumentos, técnicas e tecnologias, indicando os possíveis impactos para a segurança da informação e comunicação;

VIII - Manter contato com o Departamento de Segurança da Informação e Comunicação do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicação;

IX – Sugerir os integrantes e instituir, no âmbito do Ministério das Comunicações, a Equipe de Tratamento e Resposta a Incidentes de Segurança.

X – Sugerir a criação e seus integrantes, no âmbito do Ministério das Comunicações, da Equipe de Contingência e Continuidade de Negócios.

6. PENALIDADES

O descumprimento ou violação de um ou mais itens da POSIC ou das normas decorrentes resultará na aplicação de sanções administrativas, penais e civis cabíveis.

7. ATUALIZAÇÃO DA POSIC

Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser revisados sempre que se fizer necessário ou anualmente.

8. VIGÊNCIA

Este documento entra em vigor na data de sua publicação.