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 n° 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. 2° Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço.

Art. 3° Ficam revogadas a Portaria SPOA n° 500 de 26 de novembro de 2012, Portaria SPOA n° 519 de 13 de dezembro de 2012 e a Portaria SPOA n° 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. 1º 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. 2º 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. 3º Integram também a PoSIC as normas e os procedimentos destinados à proteger e disciplinar o uso da informação.

Art. 4º 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. 5º O cumprimento desta política de segurança e de suas normas complementares deverá ser avaliado por meio de verificações de conformidade.

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

Art. 7º 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. 8º Fica nomeado o Coordenador-Geral de Tecnologia da Informação como Gestor de Segurança da Informação e Comunicações.

Art. 9º 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.

§ 1º 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.

§ 2º 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.

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

§ 2º 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.

§ 1º 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.

§ 2º 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 n° 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

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. 3º, III, "a", da Portaria MC 89/2014.
Nº 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 **0145645** e o código CRC **985553B9**.

Criado por virginia, versão 2 por virginia em 18/09/2014 16:15:54.