Não houve publicação do Ministério Público Federal nesta seção.

ISSN 1677-7042

DIÁRIO OFICIAL DA UNIÃO

REPÚBLICA FEDERATIVA DO BRASIL • IMPRENSA NACIONAL

Ano CLVII Nº 1

Brasília - DF, quarta-feira, 2 de janeiro de 2019

SEÇÃO 1

Sumário

Presidência da República 1
Ministério da Ciência, Tecnologia, Inovações e Comunicações 5
Ministério da Cultura 9
Ministério da Defesa 9
Ministério da Educação 10
Ministério da Fazenda 23
Ministério da Justiça 32
Ministério da Saúde 33
Ministério da Segurança Pública 33
Ministério de Minas e Energia 34
Ministério do Esporte 34
Ministério dos Transportes, Portos e Aviação Civil 35
Poder Judiciário 35
Entidades de Fiscalização do Exercício das Profissões Liberais 36

Esta edição completa do DOU é composta de 36 páginas

Presidência da República

CASA CIVIL

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

PORTARIA Nº 79, DE 31 DE DEZEMBRO DE 2018

Dispõe sobre a Política de Segurança da Informação e Comunicações do Instituto Nacional de Tecnologia da Informação.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, no uso da competência prevista no art. 9º do Anexo I, do Decreto nº 8.985, de 8 de fevereiro de 2017 e considerando o disposto na Instrução Normativa nº 1 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008 e a Norma Complementar nº 3 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 30 de junho de 2009, resolve:

Art. 1º Instituir a Política de Segurança da Informação e Comunicações - POSIC no âmbito do Instituto Nacional de Tecnologia da Informação - ITI.

CAPÍTULO I
ESCOPO

Art. 2º A POSIC tem por objetivo estabelecer diretrizes, responsabilidades e competências que visam assegurar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações produzidos, processados, transmitidos, em trânsito ou armazenados sob responsabilidade do ITI.

Art. 3º Esta Política aplica-se a todos os servidores, colaboradores, estagiários e prestadores de serviço que exerçam atividades no âmbito do ITI, bem como a qualquer pessoa que venha a ter acesso aos seus ativos de informação.

Parágrafo único. Esta POSIC não se aplica aos processos de segurança da informação no âmbito da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, a qual é definida em estrutura normativa própria.

Art. 4º Os convênios, acordos e outros instrumentos congêneres celebrados pelo ITI devem atender a esta POSIC.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 5º Para fins desta Portaria entende-se por:

I . Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação da Entidade;

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

III. Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

IV. Ativos de Informação: quaisquer dados ou informações produzidos e armazenados em meio físico ou em sistemas computacionais que tenham valor para a instituição. A existência de ativos de informação implica na responsabilidade da instituição pela sua gestão;

V. Ativos físicos: equipamentos, tais como servidores de rede e equipamentos de armazenamento de dados, responsáveis pelo processamento, armazenamento e transmissão de dados no âmbito da instituição;

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;

VII. Capacitação em SIC: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC.

VIII. 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 desta entidade;

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

X . Conscientização em SIC: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema.

XI. Criticidade: grau de importância da informação;

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

XIII. 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 redes de computadores;

XIV. Gestão de Ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

XV . Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem 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;

XVI . Gestor de área: responsável pela área funcional onde a informação é criada, comunicada, manuseada, armazenada, custodiada, transportada ou descartada;

XVII . Gestor de Segurança da Informação e Comunicações: servidor responsável pelas ações de segurança da informação e comunicações no âmbito desta Entidade;

XVIII. Incidente de segurança da informação: evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores;

XIX . Informação: ativo essencial para os negócios de uma organização, que, por consequência, necessita ser adequadamente gerenciada e protegida independentemente de seu formato e meio;

XX. Integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXI. Política de Segurança da Informação e Comunicações: documento com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações nesta Entidade;

XXII. Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações neste Instituto;

XXIII. Recursos de TIC: recursos de tecnologia da informação e comunicação que processam, armazenam e transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XXIV. Risco de SIC: possibilidade de ocorrer um evento que venha a ter impacto na preservação da disponibilidade, integridade, confidencialidade e autenticidade de um ativo de informação. O risco é medido em termos de impacto e de probabilidade;

XXV. Sensibilização em SIC: atividade de ensino que tem como objetivo orientar sobre o que é Segurança da Informação e Comunicações (SIC) fazendo com que os participantes possam perceber em sua rotina pessoal e profissional ações que precisam ser corrigidas;

XXVI. 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;

XXVII. TIC: Tecnologia da Informação e Comunicação;

XXVIII. Usuário: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos ativos de informação deste Instituto;

XXIX. Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º As ações de Segurança da Informação e Comunicações - SIC do ITI deverão observar os seguintes requisitos legais e normativos:

I. 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;