PRESIDÊNCIA DA REPÚBLICA - CASA CIVIL
SCN QUADRA 02 BLOCO E - CEP 70712-905 - Brasília/DF
Telefone: (61) 3424-3875 - https://www.iti.gov.br

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. 5° 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

sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6° 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;

II. Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

III Decreto nº 7.845, de 14 de novembro 2012, que regulamenta os procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

IV. Instrução Normativa nº 1 do Gabinete de Segurança Institucional, de 13 de junho de 2008;

V. Norma Complementar nº 2 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 13 de outubro de 2008;

VI. Norma Complementar nº 3 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 30 de junho de 2009;

VII. Norma Complementar nº 9 do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional, de 15 de julho de 2014;

VIII. Portaria Normativa - ITI nº 1 de 19 de janeiro de 2012, dispõe sobre normas e procedimentos de segurança adotados nas dependências do ITI;

IX. Norma NBR ISO/IEC 27001:2013 - Sistemas de gestão da segurança da informação – Requisitos; e

X. Norma NBR ISO/IEC 27002:2013 - Código de Prática para controles de segurança da informação.

CAPÍTULO IV
PRINCÍPIOS

Art. 7° As ações relacionadas com a SIC no ITI são norteadas pelos seguintes princípios:

I. responsabilidade: os usuários devem conhecer e respeitar todas as normas de segurança da informação e comunicações do ITI;

II. clareza: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;

III. privacidade: informações relativas à intimidade, à integridade e à honra dos cidadãos devem ser resguardadas, de acordo com a legislação

vigente;

IV. celeridade: as ações de segurança da informação devem oferecer respostas tempestivas a incidentes e falhas;

V. publicidade: dar transparência no trato das informações, observados os critérios legais;

VI. legalidade: as ações de SIC levarão em consideração as leis, normas e as políticas organizacionais, administrativas, técnicas e operacionais aplicáveis ao ITI, formalmente estabelecidas; e

VII. proporcionalidade: o custo das ações de SIC não deve ser maior do que o valor do ativo da informação a ser protegido, salvo os casos formalmente analisados e justificados durante o processo de Gestão de Riscos.

CAPÍTULO V
ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Art. 8° A estrutura de Gestão de SIC no ITI compreende:

I. Gestor de Segurança da Informação e Comunicações;

II. Comitê de Segurança da Informação e Comunicações; e

III. Equipe de Tratamento e Resposta a Incidentes de Segurança - ETIR.

CAPÍTULO VI
DIRETRIZES

Seção I
Gerais

Art. 9º O ITI deverá atender as normas e legislação existentes sobre SIC, definindo normas gerais e específicas de segurança da informação, bem como procedimentos complementares, destinados à proteção da informação e à disciplina de sua utilização.

Art. 10 Devem ser estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação e comunicações, que alcancem todos os usuários do ITI, de acordo com suas competências funcionais.

Seção II
Tratamento da Informação

Art. 11 Toda informação criada, manuseada, armazenada, transportada, descartada ou custodiada é de propriedade do ITI e deve ser classificada e protegida, adequadamente, quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita.

§ 1º O usuário deve ser capaz de identificar a classificação atribuída a uma informação e, a partir desta classificação, conhecer restrições de acesso

e de divulgação associadas e obedecê-las;

§ 2º O gestor da área na qual a informação é criada quando cedida a outrem, sempre que necessário, e assessorado juridicamente, deve providenciar a documentação relativa à cessão de direitos sobre as informações do ITI, antes da sua disponibilização;

§ 3º 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. § 4º O tratamento dos dados pessoais, tais como os registros cadastrais e demais informações de cunho pessoal de cidadãos, deverá ser realizado obedecendo ao estabelecido na Lei nº 13.709/2018 (Lei de Proteção a dados pessoais).

Seção III
Tratamento de Incidentes em Rede

Art. 12 Os incidentes de SIC devem ser identificados, analisados, comunicados e tratados, em tempo hábil, de forma a impedir que evento adverso possa interferir com a perfeita execução das atividades desenvolvidas pela Entidade.

Parágrafo único. O ITI manterá ETIR formalmente instituída com estrutura e competências especificadas em norma específica.

Seção IV
Gestão de Riscos

Art. 13 Implementar e manter processo de gestão de riscos com vistas a minimizar possíveis impactos associados aos ativos de informação e comunicações. Esse processo deve possibilitar a seleção e priorização dos ativos a serem protegidos, bem como a definição e implantação de controles para a identificação e tratamento de problemas de segurança da informação. Estas medidas de proteção devem ser planejadas e os custos na aplicação de controles devem ser balanceados de acordo com os danos potenciais de falhas de segurança da informação.

Seção V
Gestão de Continuidade

Art. 14 Implementar, manter e testar periodicamente processo de gestão da continuidade de negócios visando reduzir, para um nível aceitável, o tempo de interrupção causado por desastres ou incidentes de SIC que afetem os ativos de informação e comunicações.

Seção VI
Auditoria e Conformidade

Art. 15 O cumprimento desta Política e de suas normas e procedimentos agregados devem ser auditados, periodicamente, como forma de

identificar, corrigir e/ou prevenir situações inseguras para o ITI.

Art. 16 As atividades, produtos e serviços desenvolvidos no ITI devem estar em conformidade com leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes, zelando pela proteção da privacidade das informações pessoais, profissionais e de terceiros.

Seção VII
Gestão de Ativos

Art. 17 Os ativos da organização são elementos essenciais para alcance dos objetivos institucionais, logo ações de SIC deverão garantir sua proteção. Os níveis de proteção deverão variar conforme a criticidade do ativo para o ITI.

Art. 18 Os ativos de informação devem ter controles de SIC implementados independentemente do meio em que se encontram e deverão ser protegidos contra divulgação não autorizada, modificações, remoção e destruição, a fim de evitar incidentes de segurança da informação que possam danificar a imagem institucional e interromper suas operações.

Art. 19 Os processos e atividades que sustentam serviços críticos disponibilizados pelo ITI devem ser protegidos de forma a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações.

Art. 20 Os ativos físicos de TIC deverão:

I. ser inventariados e protegidos;

II. ter identificados os seus proprietários e custodiantes;

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

IV. ter a sua entrada e saída nas dependências do ITI registradas e autorizadas por autoridade competente;

V. ser passíveis de monitoramento, respeitando os princípios legais, e ter seu uso investigado quando houver indícios de quebra de SIC por meio de mecanismos que permitam a rastreabilidade do uso desses ativos;

VI. ser regulamentados por norma específica quanto a sua utilização; e

VII. 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.

Art. 21 Os recursos tecnológicos e as instalações de infraestrutura de tecnologia da informação e comunicação devem ser protegidos contra indisponibilidade, acessos indevidos, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 22 Os sistemas de informação e as aplicações do ITI devem ser protegidos contra indisponibilidade, alterações ou acessos indevidos, falhas e interrupções não programadas.

Seção VIII

Art. 23 A autorização, o acesso e o uso das informações e dos recursos computacionais devem ser controlados e limitados ao necessário, considerando as atribuições de cada usuário e qualquer outra forma de uso ou acesso além do necessário depende de prévia autorização do gestor da área responsável pela informação.

Art. 24 Os privilégios de acesso às informações devem ser definidos pelo gestor da área responsável pela informação.

Art. 25 Ao solicitar acesso a algum ativo de informação, o solicitante deverá manifestar ciência da sua responsabilidade quanto à integridade e confidencialidade das informações a que terá acesso. O acesso somente será concedido mediante autorização do gestor da área responsável pela informação.

Art. 26 A identificação do usuário, qualquer que seja o meio e a forma, devem ser pessoal e intransferível, permitindo de maneira clara e inequívoca o seu reconhecimento.

Art. 27 Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser revistos e atualizados imediatamente, devendo ser cancelados em caso de desligamento do ITI.

Art. 28 Deverão ser mantidos procedimentos, tais como: trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação do ITI.

Art. 29 Demais regras para o Controle de Acesso serão definidas em norma(s) específica(s) em conformidade com esta POSIC e demais orientações governamentais e legislação em vigor.

Seção IX
Uso de e-mail

Art. 30 O correio eletrônico é um meio de comunicação corporativa do ITI. As regras de acesso e utilização serão definidas por norma específica, em conformidade com esta POSIC e demais orientações e diretrizes de governo.

Seção X
Acesso à Internet

Art. 31 Este acesso, no ambiente de trabalho do ITI, será regido por norma específica, em conformidade com esta POSIC e demais orientações governamentais e legislação em vigor.

Seção XI
Segurança Física e do Ambiente

Art. 32 A estrutura de Gestão de SIC do ITI deve estabelecer mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências.

As proteções devem estar alinhadas aos riscos identificados.

Art. 33 A entrada e a saída de ativos físicos de tecnologia da informação nas dependências do ITI devem ser autorizadas e registradas por autoridade competente, conforme estabelecido pela Portaria Normativa ITI nº 1 de 19 de janeiro de 2012.

Art. 34 É obrigatório o uso de crachá, carimbo ou etiqueta de identificação, independentemente da forma, deve ser pessoal e intransferível, e possibilitar de maneira clara e inequívoca o reconhecimento de seu portador, de acordo com o estabelecido pela Portaria Normativa - ITI nº 1 de 19 de janeiro de 2012.

Seção XII
Criptografia

Art. 35 Todo recurso criptográfico constitui material de acesso restrito e requer procedimentos especiais de controle para o seu acesso, manutenção, armazenamento, transferência, trânsito e descarte.

Parágrafo único. Tais procedimentos serão descritos por norma específica em conformidade com esta POSIC e legislação vigente.

Art. 36 O usuário será responsável pelo recurso criptográfico que receber.

Seção XIII
Contratos, Convênios, Acordos e Instrumentos Congêneres

Art. 37 Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC e de seus normativos decorrentes.

Art. 38 O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte divulgar esta POSIC aos seus empregados e prepostos envolvidos em atividades no ITI.

Art. 39 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.

CAPÍTULO VII
PENALIDADES

Art. 40 Todos os usuários no âmbito do ITI são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: login, crachá, token de autenticação, carimbo, endereço de correio eletrônico ou assinatura digital.

Art. 41 O desrespeito ou violação de um ou mais itens desta POSIC resultará na suspensão temporária ou permanente de privilégios de acesso aos recursos de TIC, em penas e sanções legais impostas por meio de medidas

administrativas sem prejuízo das demais medidas penais e/ou cíveis.

CAPÍTULO VIII
COMPETÊNCIAS E RESPONSABILIDADES

Art. 42 O Comitê de Governança, Riscos, Controles e Governança Digital - CGRC-GD é responsável por prover a orientação e o apoio necessários às ações de SIC, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes.

Art. 43 É de responsabilidade dos gestores das unidades administrativas do ITI zelar pelo cumprimento das diretrizes desta Política no âmbito de suas áreas de atuação.

Art. 44 O Coordenador de Tecnologia da Informação e Comunicações atuará como Gestor de Segurança da Informação e Comunicações, com as seguintes competências:

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 segurança da informação e comunicações;

IV. coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

V. realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI. manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;

VII. propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da Administração Pública Federal.

Art. 45 O Comitê de Segurança da Informação e Comunicações será integrado pelo Coordenador de Tecnologia da Informação e Comunicação (e, na sua ausência, pelo seu substituto legal) na qualidade de Gestor de SIC, e por, pelo menos, 1 (um) representante

titular e suplente indicado pelas áreas funcionais do ITI, a saber:

I. Diretoria de Auditoria, Fiscalização e Normalização;

II. Diretoria de Infraestrutura de Chaves Públicas; e

III. Coordenação Geral de Planejamento, Orçamento e Administração.

- Parágrafo único - Compete ao Comitê de Segurança da Informação e Comunicações:

I. assessorar na implementação das ações de segurança da informação e comunicações no ITI;

II. constituir grupos de trabalho para tratar de temas e propor

soluções específicas sobre segurança da informação e comunicações;

III. propor normas e procedimentos relativos à SIC no âmbito do ITI;

IV. revisar e analisar periodicamente as diretrizes e normas estabelecidas nesta política visando a sua aderência e concordância aos objetivos institucionais deste Instituto e as legislações vigentes.

Art. 46 A ETIR é responsável por:

I. coordenar as atividades de tratamento e resposta a incidentes de SIC;

II. agir proativamente com o objetivo de evitar que ocorram incidentes de SIC,

divulgando práticas e recomendações de SIC, avaliando condições de segurança de redes por meio de verificações de conformidade;

III. 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;

IV. analisar ataques e intrusões na rede do ITI;

V. executar as ações necessárias para tratar quebras de segurança;

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

VII. cooperar com outras equipes de Tratamento e Resposta a Incidentes no âmbito da Administração Pública Federal; e

VIII. participar em fóruns, redes nacionais e internacionais relativos à SIC.

Art. 47 Os usuários são responsáveis por:

I. observar o disposto nesta Portaria;

II. comunicar os incidentes que afetam a segurança dos ativos de informação à ETIR;

III. informar ao Gestor de Segurança da Informação e Comunicações qualquer tipo de ação que implique em descumprimento da POSIC; e

IV. reportar imediatamente à ETIR qualquer caso de quebra de segurança da informação por meios eletrônicos para que sejam adotadas as providências necessárias.

CAPÍTULO IX
ATUALIZAÇÃO

Art. 48 A POSIC e os normativos decorrentes devem ser revisados sempre que se fizer necessário não devendo exceder o período máximo de 3 anos.

CAPÍTULO X
VIGÊNCIA

Art. 49 Fica revogada a Portaria ITI nº 11, de 9 de março de 2012.

Art. 50 Esta Portaria entra em vigor na data de sua publicação.

GASTÃO JOSÉ DE OLIVEIRA RAMOS

Documento assinado eletronicamente por **Gastão Jose de Oliveira Ramos**, **Presidente**, em 31/12/2018, às 10:52, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 119601248669153949 7

A autenticidade deste documento pode ser conferida no site https://sei.iti.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0285645** e o código CRC **106AB179**.

Referência: Processo nº 00100.000658/2018-21 SEI nº 0285645