**MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS**

PORTARIA Nº 4 DE  DE DEZEMBRO DE 2016

Aprova a Política de Segurança da Informação e Comunicações do Ministério da Indústria, Comércio Exterior e Serviços (POSIC/MDIC).

O COMITÊ DE GOVERNANÇA DIGITAL DO MINISTÉRIO DA INDÚSTRIA, COMÉRCIO EXTERIOR E SERVIÇOS, no uso das atribuições que confere o art. 2º, inciso VII, da Portaria MDIC nº 156 de 31 de maio de 2016 e, considerando o disposto no art. 5º da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008,

R E S O L V E:

Art. 1º Aprovar a Política de Segurança da Informação e Comunicações do Ministério da Indústria, Comércio Exterior e Serviços (POSIC/MDIC).

## Capítulo I
## DAS DISPOSIÇÕES GERAIS

### Seção I
### Introdução

Art. 2º A Política de Segurança da Informação e Comunicações (POSIC) tem por finalidade estabelecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações no âmbito do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) e, no que couber, do relacionamento desta Pasta com outros órgãos públicos ou entidades privadas.

§ 1º A POSIC integra o arcabouço legal do Sistema de Gestão de Segurança da Informação e Comunicações (SGSIC) do MDIC.

§ 2º As Normas Complementares (NC) à POSIC, partes integrantes desta política, emanam dos princípios e diretrizes deste normativo.

Art. 3º Para efeitos desta norma, entende-se por:

I - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

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

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

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

V - 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;

VI - aceitar o risco: uma forma de tratamento de risco na qual a Alta Administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado;

VII - acesso remoto assistido: tecnologia que permite que um computador seja manuseado por meio de outro, de forma que o usuário do computador acessado possa acompanhar as ações executadas;

VIII - ativo de informação: é um ativo essencial para o MDIC e, por consequência, necessita ser adequadamente gerenciado e protegido, independentemente de seu formato e meio;

IX - ciclo PDCA (**plan, do, check, act**): método de gestão baseado em quatro etapas: Planejamento, Execução, Avaliação e Ação Corretiva;

X - classificação da informação: consiste em classificar a informação quanto ao grau de sigilo, em consonância com a legislação vigente, e buscar o estabelecimento do controle de segurança devido a cada informação tratada ou custodiada pelo MDIC ao longo do seu ciclo de vida;

XI - colaborador: todas as pessoas envolvidas com o desenvolvimento de atividades no MDIC de caráter permanente, continuado ou eventual, incluindo autoridades, servidores, prestadores de serviço, consultores e estagiários;

XII - diretrizes de segurança da informação e comunicações: ações que definem a Política de Segurança da Informação e Comunicações do MDIC (POSIC/MDIC), visando a preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações da Instituição;

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 Computacionais, conforme estabelecido na Norma Complementar 01;

XIV - gestor de segurança da informação e comunicações (GSIC): servidor público efetivo responsável pelas ações de segurança da informação e comunicações do MDIC, conforme estabelecido na IN GSI/PR nº 1;

XV - gestor de segurança e credenciamento: responsável pela segurança da informação classificada em qualquer grau de sigilo no órgão de registro e posto de controle

XVI - incidente de segurança da informação: evento indesejado ou inesperado, com probabilidade de comprometer as operações do negócio e ameaçar um ativo de informação;

XVII - incidentes de segurança da tecnologia da informação: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

XVIII - logs: arquivos usados para registrar ações no ambiente de Tecnologia da Informação e Comunicação (TIC), resultando em fontes de informação para rastreio e futuras auditorias;

XIX - proprietário da informação: refere-se à parte interessada do MDIC ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência da informação.

XX - público-alvo: todos os colaboradores que, direta ou indiretamente, tenham acesso a informações do MDIC;

XXI - quebra de segurança: ação ou omissão, intencional ou acidental, que resulte no comprometimento da segurança da informação e comunicações;

XXII - recursos de Tecnologia da Informação: conjunto formado pelos bens e serviços de tecnologia da informação que constituem a infraestrutura utilizada na produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação da informação;

XXIII - reduzir o risco: forma de tratamento de risco na qual o gestor decide realizar determinada atividade para reduzir a probabilidade de ocorrência do risco ou as suas consequências negativas;

XXIV - responsável pelo ativo de informação: servidor público responsável pela salvaguarda do ativo de informação;

XXV - risco: é um evento hipotético, que possui chance de ocorrência futura, e cuja ocorrência pode afetar uma organização de maneira positiva ou negativa, e gerar impacto ou oportunidade significante;

XXVI - risco de segurança da informação: possibilidade de uma ameaça explorar uma vulnerabilidade na gestão de um ativo de informação de modo a causar prejuízo à organização;

XXVII - servidor público: toda pessoa legalmente investida em cargo público;

XXVIII - tolerância a risco: percentual de riscos que o órgão está disposto a assumir;

XXIX - transferir o risco: forma de tratamento de risco na qual o gestor decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

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

XXXI - tratamento dos riscos: processo e implementação de ações, controles ou medidas para evitar, reduzir, aceitar ou transferir um risco;

XXXII - usuário: colaboradores que utilizam recursos de TIC do Ministério;

XXXIII - usuário externo: todas as pessoas não caracterizadas como colaborador e que utilizam recursos de TIC do Ministério em caráter eventual;

XXXIV - vulnerabilidades: fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, e podem ser corrigidas ou evitadas por uma ação interna de segurança da informação.

§ 1º As diretrizes de segurança da informação e comunicações previstas nesta POSIC e nas NC são aplicadas no âmbito do MDIC a todos os colaboradores que tenham acesso às informações e aos recursos de Tecnologia da Informação deste Ministério.

§ 2º Toda e qualquer informação gerada, transformada, adquirida, recebida, utilizada ou armazenada pela organização é considerada parte do patrimônio do MDIC e deve ser adequadamente protegida, segundo as diretrizes descritas neste documento e demais regulamentações complementares em vigor, obedecendo aos princípios da disponibilidade, integridade, confiabilidade e autenticidade;

## Seção II
## Dos Objetivos

Art. 4º A POSIC tem como objetivos:

I - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação e comunicações.

II - estabelecer diretrizes de controle a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

III - estabelecer orientações gerais de segurança da informação e comunicações e, desta forma, preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações.

Parágrafo único. Esta POSIC será divulgada amplamente a fim de promover a cultura de segurança da informação e comunicações.

## Seção III
## Do Comprometimento

Art. 5º A alta administração do MDIC está comprometida com o desenvolvimento e com a implementação do SGSIC, visando a proteger todos os ativos de informação.

Parágrafo único. A POSIC é instituída pelo Comitê de Governança Digital – CGD, a quem cabe estabelecer, regulamentar, por meio de Normas Complementares, e rever, quando necessário, seus princípios e diretrizes, alocar os recursos necessários à sua implementação de forma sistêmica e integrada aos negócios, respaldando a realização de auditorias e a aplicação de ações preventivas e corretivas.

**Seção V**
**Dos Princípios**

Art. 6º Esta POSIC rege-se pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, em destaque:

I - continuidade dos processos e serviços essenciais para o funcionamento deste Ministério;

II - responsabilidade dos colaboradores, constituída no dever de conhecer e respeitar a POSIC do Ministério e suas Normas Complementares;

III - publicidade da informação, salvo quando estritamente necessário para assegurar a privacidade e a intimidade do cidadão, ou para garantir a segurança do Estado e da sociedade, nos termos da lei;

IV - disponibilidade, integridade, confidencialidade e autenticidade das informações e das comunicações;

**Capítulo II**
**Das Diretrizes**

**Seção I**
**Diretrizes Gerais**

Art. 7º Esta POSIC possui as seguintes diretrizes gerais:

I - tratamento da informação:

a) toda informação deve ser tratada de acordo com sua classificação de segurança;

b) toda informação deve ser transportada, preservada e descartada com segurança física e lógica compatível com sua classificação;

c) todo colaborador deve fazer uso da informação apenas no que concerne às atribuições de interesse do MDIC e no limite de suas competências;

d) o MDIC se reserva ao direito de monitorar o uso e a custódia das suas informações, bem como o uso de seus recursos de informação;

e) todo ativo de informação deve possuir um gestor e ao menos um responsável;

f) as informações institucionais não devem ser expostas na presença de pessoas não autorizadas; e

g) a autorização, o acesso e o uso da informação e dos ativos de informação são controlados e limitados às atribuições necessárias e suficientes para cumprimento das atividades de cada colaborador, exceto se houver prévia autorização do proprietário da informação.

II - tratamento de incidentes de segurança da informação:

a) deve ser instituída Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), que terá a responsabilidade de receber, analisar e responder às notificações e atividades relacionados a incidentes de segurança da tecnologia da informação; e

b) a ETIR deve ser imediatamente comunicada dos incidentes de segurança, tais como indícios de fraude, sabotagem ou falha na segurança em processos, sistemas, instalações ou equipamentos.

III - gestão de risco:

a) o processo de Gestão de Riscos de Segurança da Informação e Comunicações deverá considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do MDIC, além de estar alinhado a esta Política de Segurança da Informação e Comunicações; e

b) o processo de Gestão de Riscos de Segurança da Informação e Comunicações deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação e Comunicações.

IV - gestão de continuidade: os recursos necessários para garantir a integridade e a disponibilidade das informações do MDIC têm que ser suportados por um plano de continuidade dos Recursos de Tecnologia da Informação para reduzir a um nível aceitável a possibilidade de interrupção causada por desastres ou falhas nos recursos que suportam os processos de negócio deste Ministério, devendo ser testado, revisado e documentado conforme a necessidade;

V - auditoria e conformidade:

a) devem ser definidos critérios de auditoria com o intuito de aferir o cumprimento desta POSIC, suas Normas Complementares e Procedimentos;

b) devem ser estabelecidos critérios de salvaguarda de **logs** dos ativos de tecnologia da informação e comunicações, a fim de possibilitar auditoria; e

c) deve ser continuamente avaliada a conformidade desta POSIC com a legislação vigente, no que diz respeito a Gestão de Segurança da Informação e Gestão de Tecnologia da Informação.

VI - controles de acesso:

a) as credenciais de acesso de colaborador são pessoais e intransferíveis;

b) os privilégios de acesso às informações devem ser definidos pelo proprietário da informação; e

c) somente é permitido o uso de ativos de informação autorizados pelo MDIC, exclusivamente para a finalidade pretendida pela organização, e que estejam de acordo com a legislação em vigor.

VII - uso de e-mail e internet: o uso dos Recursos de TI, em qualquer de suas formas, deverá se restringir à esfera profissional e seu conteúdo deverá se ater às atribuições desempenhadas por cada colaborador, observando-se sempre a conduta ética e os bons costumes.

## Seção II
## Das Penalidades

Art. 8º Todos os colaboradores da organização estão sujeitos às regras desta POSIC e devem observar integralmente o que dispõe este documento. A inobservância dessas regras ou a violação desta POSIC acarretará a apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização penal, civil e administrativa.

## Seção III
## Das Competências e Responsabilidades

Art. 9º Cabe ao MDIC divulgar esta POSIC, suas Normas Complementares e respectivas atualizações a todos os colaboradores do órgão.

Art. 10º Cabe ao colaborador do MDIC:

I - cumprir fielmente as políticas, as normas, os procedimentos e as orientações de segurança da informação e comunicações do MDIC;

II - buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;

III - assinar Termo de Responsabilidade, que formalizará a ciência e o aceite da Política de Segurança da Informação e Comunicações do MDIC (POSIC/MDIC), bem como estabelecerá responsabilidade pessoal por seu cumprimento;

IV - proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pelo Ministério;

V - assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Ministério; e

VI - comunicar imediatamente ao Comitê de Segurança da Informação e Comunicações (CSIC) qualquer descumprimento ou violação desta Política e/ou de seus documentos complementares.

Art. 11. O MDIC deverá possuir estrutura organizacional formalmente instituída, com responsabilidade de executar os processos de segurança da informação, que deverá conter, no mínimo:

I - Comitê de Governança Digital – CGD;

II - Gestor de Segurança da Informação e Comunicações;

III - Gestor de Segurança e Credenciamento;

III - Comitê de Segurança da Informação e Comunicações – CSIC; e

IV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR.

Parágrafo único. A atuação dos componentes acima será definida em norma expedida pelo CGD.

**Seção IV**
**Da Revisão, Atualização e Divulgação**

Art. 12. Esta POSIC deve ser revisada e atualizada:

I - anualmente;

II - tempestivamente, na ocorrência de novos eventos ou fatos relevantes, tais como:

a) surgimento ou alteração de leis ou regulamentações vigentes;

b) mudança estratégica da instituição;

c) expiração da data de validade do documento;

d) mudanças de tecnologia na organização; ou

e) atualização das boas práticas em Segurança da Informação e Comunicação.

**Capítulo III**
**Disposições Finais**

Art. 13. As dúvidas sobre a Política de Segurança da Informação e Comunicações e seus documentos devem ser submetidas ao Comitê de Segurança da Informação e Comunicações.

Art. 14. O investimento necessário em medidas de segurança deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos para o negócio, a atividade fim e os objetivos institucionais.

Art. 15. Os colaboradores devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições de modo a minimizar possíveis riscos à segurança.

Art. 16. Esta norma foi elaborada em conformidade às seguintes referências legais e normativas:

I - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações;

II - 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;

III - Decreto nº 7.724, de 16 de maio de 2012, que regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo, conforme o disposto na Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição;

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

V - Decreto nº 8.638, de 15 de janeiro de 2016, que institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

VI - Decreto nº 8.917, de 29 de novembro de 2016, que que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Indústria, Comércio Exterior e Serviços, remaneja cargos em comissão e funções gratificadas, substitui cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS por Funções Comissionadas do Poder Executivo - FCPE e altera o Decreto nº 8.854, de 22 de setembro de 2016, que aprova a Estrutura Regimental do Instituto Nacional da Propriedade – INPI;

VII - Instrução Normativa Nº 1 GSI/PR, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicação na Administração Pública Federal;

VIII - Normas Complementares à IN Nº 01 GSI/PR/2008;

IX - ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação;

XI - ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação; e

XII - ABNT NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

Art. 18 - Esta Portaria entra em vigor na data de sua publicação.

Art. 19. Fica revogada a Portaria SPOA nº 4, de 23 de janeiro de 2013.

MARCOS JORGE DE LIMA
Presidente do Comitê de Governança Digital