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 40, DE 28 DE JUNHO DE 2018

Institui a Política de Gestão de Riscos do Instituto Nacional de Tecnologia da Informação – ITI.

O **DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI**, autarquia vinculada à Casa Civil da Presidência da República, no uso das atribuições, e considerando o disposto no art. 17 da Instrução Normativa Conjunta CGU/MP n° 01, de 10 de maio de 2016 e Decisão do Comitê de Governança, Riscos, Controles e de Governança Digital – CGRC-GD de 19 de junho de 2018,

**RESOLVE:**

Art. 1º Aprovar a Política de Gestão de Riscos do Instituto Nacional de Tecnologia da Informação – ITI, na forma do Anexo I desta Portaria, disponível em http://www.iti.gov.br

Art. 2º Esta portaria entra em vigor na data de sua publicação.

**GASTÃO JOSÉ DE OLIVEIRA RAMOS**

## ANEXO I

### CAPÍTULO I

### DISPOSIÇÕES GERAIS

Art. 1° Fica instituída a Política de Gestão de Riscos do Instituto Nacional de Tecnologia da Informação – ITI.

Art. 2° Para fins desta Portaria, considera-se:

I – Ameaça: algo que oferece risco a um ativo da organização.

II – Apetite ou tolerância ao risco: nível de risco que uma organização está disposta a aceitar na consecução de seus objetivos e finalidade;

III – Autoridades Competentes: representantes da alta gestão da organização, que devem aprovar pontos importantes relativos à gestão de riscos e prover os recursos necessários;

IV – Ativo: é tudo que tem valor para a organização;

V – Ativos de valor para a Organização:

a) Pessoas

b) Informações

c) Processos de Negócio e

d) Soluções de Tecnologia da Informação e Comunicação.

VI – Controle: forma de gerenciar o risco, incluindo adoção de políticas, procedimentos, diretrizes, práticas, estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

VII – Controle Interno da Gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança para o alcance dos objetivos organizacionais;

VIII – Evento: um ou mais incidentes ou ocorrências, proveniente do ambiente interno ou externo, ou mudança em um conjunto específico de circunstâncias, podendo consistir em algo não acontecer;

IX – Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

X – Meta: alvo ou propósito com que se define um objetivo a ser alcançado;

XI – Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

XII – Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;

XIII – Gerenciamento de risco: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança no alcance dos objetivos organizacionais;

XIV – Gestão de Riscos: arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente;

XV – Gestor de Risco: pessoa ou estrutura organizacional com autoridade e responsabilidade para gerenciar risco;

XVI – Nível de Risco: medida de importância ou significância do risco, considerando a probabilidade de ocorrência do evento e o seu impacto nos objetivos;

XVII – Objeto de Gestão de Risco: qualquer processo de trabalho, atividade, projeto, iniciativa ou ação de plano institucional, assim como os recursos que dão suporte à realização dos objetivos institucionais do ITI;

XVIII – Oportunidade: possibilidade de que um evento afete positivamente o alcance de objetivos;

XIX – Organização Estendida: conjunto de organizações que executam atividades relacionadas à cadeia de valor para obtenção do produto final pelos usuários. Fazem parte da Organização Estendida o ITI, as entidades credenciadas e outras organizações dentro e fora do governo, a exemplo das entidades fiscalizadoras superiores, outros órgãos públicos e fornecedores.

XX – Resposta a Risco: qualquer ação adotada para lidar com risco, podendo consistir em:

a) aceitar o risco por uma escolha consciente;

b) transferir ou compartilhar o risco a outra parte;

c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que origina o risco ou;

d) mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências.

XXI – Risco: possibilidade de ocorrência de um evento que tenha impacto no atingimento dos objetivos da organização;

XXII – Risco-Chave: risco que, em função do impacto potencial ao ITI ou à ICP – Brasil, deve ser conhecido pela alta administração;

XXIII – Risco Inerente: risco a que uma organização está exposta sem considerar quaisquer medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

XXIV – Risco Residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;

XXV – Vulnerabilidade: ponto falho ou "fraqueza" de um determinado ativo ou controle que pode ser explorado por uma ameaça;

XXVI – Incerteza: estado, mesmo que parcial, da deficiência de informações relacionadas a um evento, sua compreensão, seu conhecimento, sua consequência, ou sua probabilidade. A incerteza pode se transformar em ameaça ou oportunidade para a organização.

## CAPÍTULO II

## DOS PRINCÍPIOS

Art. 3° *A* Gestão de Riscos tem como objetivo auxiliar na tomada de decisão com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais, devendo observar os seguintes princípios:

I – fomentar a inovação e a ação empreendedora responsável;

II – considerar riscos e oportunidades;

III – aplicar-se a qualquer tipo de atividade ou projeto;

IV – basear-se nas melhores informações disponíveis;

V – aplicar-se de forma contínua e integrada aos processos de trabalho e ser parte integrante dos processos organizacionais;

VI – ser implantada por meio de ciclos de revisões e melhoria contínua;

VII – subsidiar a tomada de decisões;

VIII – considerar a importância dos valores humanos e culturais;

IX – agregar valor e proteger o ambiente interno do ITI;

X – ser transparente e inclusiva;

XI – abordar explicitamente a incerteza;

XII – ser dinâmica, interativa e capaz de reagir a mudanças; e

XIII – ser dirigida, apoiada e monitorada pela alta administração.

## CAPÍTULO III

## DOS OBJETIVOS

Art. 4° A Gestão de Riscos tem por objetivos:

I – aumentar a probabilidade de atingimento dos objetivos do ITI;

II – fomentar uma gestão proativa;

III – atentar para a necessidade de se identificar e tratar riscos em todo o ITI;

IV – facilitar a identificação de oportunidades e ameaças;

V – prezar pelas conformidades legal e normativa dos processos organizacionais;

VI – melhorar a prestação de contas à sociedade;

VII – melhorar a governança;

VIII – estabelecer uma base confiável para a tomada de decisão e o planejamento;

IX – melhorar o controle interno da gestão;

X – alocar e utilizar eficazmente os recursos para o tratamento de riscos;

XI – melhorar a eficácia e a eficiência operacional;

XII – melhorar a prevenção de perdas e a gestão de incidentes;

XIII – minimizar perdas;

XIV – melhorar a aprendizagem organizacional; e

XV – aumentar a capacidade da organização de se adaptar a mudanças.

Art. 5° O processo de gestão de riscos no ITI deve observar:

I – o ambiente interno, o ambiente externo e a organização estendida;

II – os objetivos estratégicos, táticos e operacionais;

III – a razoabilidade da relação custo-benefício nas ações para tratamento de riscos;

IV – a comunicação tempestiva sobre riscos às partes interessadas; e

V – o acompanhamento dos riscos-chave pela alta administração.

Parágrafo único. A Gestão de Riscos deverá estar integrada aos processos de planejamento estratégico, tático e operacional, à gestão e à cultura organizacional do ITI. Nas atividades de planejamento, considera-se, sempre que couber, o risco como um dos critérios para seleção e priorização de iniciativas e ações.

Art. 6° O gerenciamento de riscos deverá ser implementado de forma gradual em todas as áreas do ITI, sendo priorizados os processos organizacionais que impactam diretamente no atingimento dos objetivos estratégicos definidos no Planejamento Estratégico do ITI.

## CAPÍTULO IV

## DA OPERACIONALIZAÇÃO

Art. 7° O processo de Gestão de Riscos e do ITI contempla o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento de riscos, a comunicação e consulta com partes interessadas, o monitoramento e a melhoria contínua.

Art. 8° A operacionalização da Gestão de Riscos deverá ser descrita pela Metodologia de Gestão de Riscos do ITI, que deverá contemplar, no mínimo, as seguintes etapas:

I – entendimento do contexto: etapa em que são identificados os objetivos relacionados ao processo organizacional e definidos os contextos externo e interno a serem levados em consideração ao gerenciar riscos;

II – identificação de riscos: etapa em que são identificados possíveis riscos para objetivos associados aos processos organizacionais;

III – análise de riscos: etapa em que são identificadas as possíveis causas e consequências do risco;

IV – avaliação de riscos: etapa em que são estimados os níveis dos riscos identificados;

V – priorização de riscos: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;

VI – definição de respostas aos riscos: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis ao apetite estabelecido para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas;

VII – comunicação e monitoramento: etapa que ocorre durante todo o processo de gerenciamento de riscos e é responsável pela integração de todas as instâncias envolvidas, bem como pelo monitoramento contínuo da própria Gestão de Riscos, com vistas a sua melhoria; e

VIII – as áreas definidas na organização deverão identificar seus ativos, bem como possíveis ameaças, vulnerabilidades e os respectivos controles.

Parágrafo único. A Metodologia de Gestão de Riscos deverá contemplar critérios predefinidos de avaliação, de forma a permitir a comparabilidade entre os riscos.

## CAPÍTULO V

## DAS COMPETÊNCIAS

Art. 9° Compete ao Comitê de Governança, Riscos, Controles e Governança Digital – CGRC-GD, as atribuições instituídas pela Portaria n° 33, de 20 de junho de 2017:

I – definir e atualizar as estratégias de implementação da Gestão de Riscos, considerando os contextos externo e interno;

II – definir os níveis de apetite a risco dos processos organizacionais;

III – definir os responsáveis pelo gerenciamento de riscos dos processos organizacionais;

IV – aprovar a periodicidade máxima do ciclo do processo de gerenciamento de riscos para cada um dos processos organizacionais;

V – aprovar as respostas e as respectivas medidas de controle a serem implementadas nos processos organizacionais;

VI – aprovar a Metodologia de Gestão de Riscos e suas revisões;

VII – aprovar os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;

VIII – garantir o apoio institucional para promover a Gestão de Riscos, em especial os seus recursos, o relacionamento entre as partes interessadas e o desenvolvimento contínuo dos servidores; e

IX – propiciar o alinhamento da gestão de riscos aos padrões de ética e de conduta do ITI.

Art. 10. Compete aos Gestores de Risco:

I – construir e propor ao CGRC-GD os indicadores de desempenho para a Gestão de Riscos, alinhados com os indicadores de desempenho do ITI;

II – prover as informações necessárias à Gestão de Risco para Auditoria Interna;

III – assegurar que o risco seja gerenciado de acordo com a política de gestão de riscos da organização;

IV – monitorar o risco ao longo do tempo, de modo a garantir que as respostas adotadas resultem na manutenção do risco em níveis adequados, de acordo com a política de gestão de riscos; e

V – garantir que as informações adequadas sobre o risco estejam disponíveis em todos os níveis da organização.

Art. 11. Compete à Auditoria Interna:

I) oferecer avaliações e assessoramento ao CGRC-GD, destinadas ao aprimoramento dos controles internos, de forma que controles mais eficientes e eficazes mitiguem os principais riscos de forma a propiciar o alcancem dos objetivos;

II – monitorar a aplicação da Política de Gestão de Riscos;

IV – propor melhorias nos controles de gerenciamento de riscos objetivando a efetividade dos processos;

V – monitorar as recomendações e orientações deliberadas pelo CGRC-GD;

VI – monitorar a execução do processo de Gestão de Riscos e os resultados por ele produzidos;

VIII – medir o desempenho da Gestão de Riscos objetivando a sua melhoria contínua;

Art. 12. Compete à Coordenação-Geral de Planejamento, Orçamento e Administração, por meio da Coordenação de Planejamento, Orçamento e Modernização Institucional – COPOM:

I – manter a Metodologia de Gestão de Riscos atualizada e aderente às melhores práticas;

II – participar da definição de requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;

III – subsidiar o Comitê de Governança de Riscos no que se refere à prestação de informações relativas ao gerenciamento dos riscos;

IV – apoiar os Gestores de Riscos e as Unidades responsáveis pelo gerenciamento de riscos dos processos quanto à aplicação da metodologia;

V – assegurar que o gerenciamento de riscos esteja aderente ao Plano Estratégico e à Gestão de Processos;

VI – consolidar os resultados das diversas áreas em relatórios gerenciais e encaminhá-los ao CGRC-GD;

VII – elaborar, em parceria com a Assessoria de Comunicação – ASCOM, o Plano de Comunicação de Gestão de Riscos;

Art. 13. Compete às Unidades responsáveis pelo gerenciamento de riscos dos processos:

I – identificar, analisar e avaliar os riscos dos processos sob sua responsabilidade, em conformidade ao que define esta política;

II – propor respostas e respectivas medidas de controle a serem implementadas nos processos organizacionais sob sua responsabilidade;

III – monitorar a evolução dos níveis de riscos e a efetividade das medidas de controles implementadas nos processos organizacionais sob sua responsabilidade;

IV – informar à Auditoria Interna sobre mudanças significativas nos processos organizacionais sob sua responsabilidade, assim como apresentar relatórios gerenciais periódicos com vistas a consolidação dos resultados;

V – responder às requisições da Auditoria Interna; e

VI – disponibilizar as informações adequadas quanto à gestão dos riscos dos processos sob sua responsabilidade a todos os níveis do ITI e demais partes interessadas.

Parágrafo único. Os responsáveis pelo gerenciamento de riscos dos processos organizacionais devem ter alçada suficiente para orientar e acompanhar as etapas de identificação, análise, avaliação e implementação das respostas aos riscos.

Art. 14. Compete a todos os servidores do ITI o monitoramento da evolução dos níveis de riscos e da efetividade das medidas de controles implementadas nos processos organizacionais em que estiverem envolvidos ou que tiverem conhecimento.

Parágrafo único. No monitoramento de que trata o caput deste artigo, caso sejam identificadas mudanças ou fragilidades nos processos organizacionais, o servidor deverá reportar imediatamente o fato ao responsável pelo gerenciamento de riscos do processo em questão.

## CAPÍTULO VI

## DAS DISPOSIÇÕES FINAIS

Art. 15. O CGRC-GD, e as demais áreas responsáveis pelo gerenciamento de riscos dos processos organizacionais deverão manter fluxo regular e constante de informações entre si.

Art. 16. As iniciativas relacionadas à Gestão de Riscos existentes no ITI anteriormente à publicação desta Portaria deverão ser gradualmente alinhadas à Metodologia de Gestão de Riscos aprovada pelo Comitê de Governança, Riscos, Controles e Governança Digital.

§1° A Metodologia de Gestão de Riscos deverá ser aprovada em até 90 (noventa) dias após a publicação desta política.

§2° O alinhamento de que trata o caput deste artigo deve ser feito no prazo máximo de 12 (doze) meses após a aprovação da Metodologia de Gestão de Riscos.

Art. 17. A política de gestão de riscos do Instituto Nacional de Tecnologia da Informação será revista sempre que necessário, no intuito de mantê-la atualizada diante de mudanças no ambiente interno ou externo.

Art. 18. Os casos omissos ou as excepcionalidades serão resolvidos pelo comitê CGRC-GD.

---

Documento assinado eletronicamente por **Gastão Jose de Oliveira Ramos**, **Presidente**, em 28/06/2018, às 17:27, 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: 1196012486691539497

---

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 **0162243** e o código CRC **8E768CBA**.

---