

## RESOLUÇÃO

|                                     |                             |
|-------------------------------------|-----------------------------|
| IDENTIFICAÇÃO<br><b>RI-020/2016</b> | FOLHA (Nº/DE)<br><b>1/1</b> |
|-------------------------------------|-----------------------------|

|  |
|--|
| VIGÊNCIA<br><b>INÍCIO: 01/12/2016 FIM:</b> |
|--|

|  |                                    |
|--|------------------------------------|
| TÍTULO<br><b>POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLE INTERNO e CONFORMIDADE</b>                             |                                    |
| REFERÊNCIAS<br><b>TEMA:</b> Riscos Empresariais<br><b>PALAVRAS-CHAVE:</b> política, controle interno, gestão de riscos |                                    |
| CÓDIGO DE CLASSIFICAÇÃO<br><b>010</b>  | GRAU DE SIGILO<br><b>Ostensivo</b> |

**A DIRETORA-PRESIDENTE**, no uso das atribuições que lhe confere o art.11 do Estatuto Social do SERPRO, aprovado pelo Decreto nº 6.791, de 10 de março de 2009,

### RESOLVE:

**1.0** Atualizar a Política Corporativa de Gestão de Riscos, Controle Interno e Conformidade, conforme Anexo 1, instituída pela Resolução RI-014/2016, de 13 de outubro de 2016, com o objetivo de estabelecer o direcionamento estratégico da Gestão de Riscos, Controle Interno e Conformidade para o SERPRO.

**2.0** A atualização é decorrente de Relatório da Auditoria de Integridade do Ministério da Transparência, Fiscalização e Controle (MTFC), que emitiu sugestões de melhoria para a política de gestão de riscos corporativos.

**3.0** Substituir a Resolução RI-014/2016, de 13 de outubro de 2016.

Brasília, 01 de dezembro de 2016

**MARIA DA GLÓRIA GUIMARÃES DOS SANTOS**  
Diretora-Presidente

DIGOG/SUPCR/rdpl

Documento assinado com certificado digital em conformidade com a Medida Provisória nº 2200-2/2001. Sua autenticidade pode ser confirmada no endereço <<http://www.serpro.gov.br/assinador-digital>>.

[www.serpro.gov.br](http://www.serpro.gov.br)

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 1/7          |
| TÍTULO  |        |           |               |        |              |
| POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE |        |           |               |        |              |

## 1.0 OBJETIVO

Estabelecer o direcionamento estratégico e determinações para as atividades corporativas de gestão de riscos, controles internos e conformidade, de forma a assegurar sua integração aos processos organizacionais, reduzir a exposição a riscos, danos ao patrimônio e à imagem empresarial; além de fortalecer os mecanismos de governança e o alcance dos objetivos estratégicos do SERPRO.

## 2.0 ÂMBITO DE APLICAÇÃO

Todas as Unidades organizacionais.

## 3.0 DEFINIÇÕES

A fonte principal das definições é a INSTRUÇÃO NORMATIVA CONJUNTA Nº 1, da Controladoria Geral da União (CGU) e do Ministério do Planejamento (MP), de 10 de maio de 2016, com adaptações para o SERPRO.

**a) Ambiente de controle:** é a base de todos os controles internos da gestão, sendo formado pelo conjunto de regras e estrutura que determinam a qualidade dos controles internos da gestão. O ambiente de controle deve influenciar a forma pela qual se estabelecem as estratégias e os objetivos e na maneira como os procedimentos de controle interno são estruturados. Alguns dos elementos do ambiente de controle são:

- a1) integridade pessoal e profissional e valores éticos assumidos pela direção e pelo quadro de servidores,
- a2) comprometimento para reunir, desenvolver e manter colaboradores competentes,
- a3) filosofia da direção e estilo gerencial, com clara assunção da responsabilidade de supervisionar os controles internos da gestão,
- a4) estrutura organizacional na qual estejam claramente atribuídas responsabilidades e delegação de autoridade, para que sejam alcançados os objetivos da organização ou das políticas públicas, e
- a5) políticas e práticas de recursos humanos, especialmente a avaliação do desempenho e prestação de contas dos colaboradores pelas suas

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 2/7          |
| TÍTULO  |        |           |               |        |              |
| POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE |        |           |               |        |              |

responsabilidades pelos controles internos da gestão da organização ou política pública.

**b) Componentes dos controles internos da gestão:** são o ambiente de controle interno da entidade, a avaliação de risco, as atividades de controles internos, a informação e comunicação e o monitoramento;

**c) Controles internos da gestão:** conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada pela direção e pelo corpo de servidores das organizações, destinados a enfrentar os riscos e fornecer segurança razoável de que, na consecução da missão da entidade, os seguintes objetivos gerais serão alcançados:

- c1) execução ordenada, ética, econômica, eficiente e eficaz das operações,
- c2) cumprimento das obrigações de accountability,
- c3) cumprimento das leis e regulamentos aplicáveis, e
- c4) salvaguarda dos recursos para evitar perdas, mau uso e danos, e
- c5) estabelecimento de controles internos no âmbito da gestão pública visa essencialmente aumentar a probabilidade de que os objetivos e metas estabelecidos sejam alcançados, de forma eficaz, eficiente, efetiva e econômica.

**d) Conformidade:** agir de acordo com uma regra; estar em concordância com as leis e os regulamentos externos e internos;

**e) Fraude:** quaisquer atos ilegais caracterizados por desonestidade, dissimulação ou quebra de confiança. Estes atos não implicam o uso de ameaça de violência ou de força física;

**f) Gerenciamento de riscos:** processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos da organização;

**g) Governança:** combinação de processos e estruturas implantadas pela alta administração, para informar, dirigir, administrar e monitorar as atividades da organização, com o intuito de alcançar os seus objetivos;

**h) Governança no setor público:** compreende essencialmente os mecanismos de liderança, estratégia e controle postos em prática para avaliar, direcionar e monitorar a atuação da gestão, com vistas à condução de políticas públicas e à

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 3/7          |
| TÍTULO  |        |           |               |        |              |
| POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE |        |           |               |        |              |

prestação de serviços de interesse da sociedade;

**i) Incerteza:** incapacidade de saber com antecedência a real probabilidade ou impacto de eventos futuros;

**j) Mensuração de risco:** significa estimar a importância de um risco e calcular a probabilidade e o impacto de sua ocorrência;

**k) Política de gestão de riscos:** declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos;

**l) Risco:** possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

**m) Risco inerente:** risco a que uma organização está exposta sem considerar quaisquer ações gerenciais que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

**n) Risco residual:** risco a que uma organização está exposta após a implementação de ações gerenciais para o tratamento do risco;

**o) Riscos financeiros / orçamentários:** eventos que podem comprometer a capacidade do órgão ou entidade de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de licitações;

**p) Riscos de imagem/reputação do órgão:** eventos que podem comprometer a confiança da sociedade (ou de parceiros, de clientes ou de fornecedores) em relação à capacidade do órgão ou da entidade em cumprir sua missão institucional.

**q) Riscos legais:** eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades do órgão ou entidade;

**r) Riscos operacionais:** eventos internos e externos que podem comprometer as atividades do órgão ou entidade, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas de informação;

**s) Tipologia de Riscos:** forma de classificação dos riscos, de acordo com tipos específicos, para facilitar seu agrupamento e avaliação pela organização. No caso do Serpro serão considerados os tipos: riscos operacionais, riscos de imagem/reputação do órgão, riscos legais e os riscos financeiros/orçamentários; e

**t) Tolerância ao risco:** nível de risco que uma organização está disposta a aceitar.

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 4/7          |
| TÍTULO  |        |           |               |        |              |
| POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE |        |           |               |        |              |

#### 4.0 PREMISSAS

4.1 A gestão de riscos, os controles internos e conformidade são mecanismos de governança e de tomada de decisão, cuja finalidade é facilitar o alcance dos objetivos organizacionais.

4.2 O comprometimento da alta direção, evidenciado pelo apoio inequívoco, é garantia da independência na execução dos mecanismos previstos nesta política.

4.3 A gestão de riscos, os controles internos e a conformidade são parte integrante de todos os processos organizacionais.

4.4 Todos os gestores e empregados são responsáveis pela gestão de riscos, controles internos e conformidade em seus processos de atuação, bem como por alocar recursos para este fim, e serão orientados para o uso dos instrumentos normativos e procedimentos para executar estas tarefas.

4.5 A organização da gestão de riscos, dos controles internos e conformidade é estabelecida e mantida em ciclos de melhoria, para permitir ajustes e sua adaptação às mudanças organizacionais.

#### 4.6 Esta política abrange:

**a) Riscos operacionais:** vinculados a processos internos, pessoas, infraestrutura e sistemas de informação - além dos riscos de imagem e legais; e

**b) Riscos estratégicos:** relacionados ao planejamento estratégico da organização.

4.7 Esta política é complementada pelas medidas e práticas do Programa de Integridade do Serpro voltadas ao combate dos desvios de fraude e corrupção.

#### 5.0 DETERMINAÇÕES

5.1 A gestão de riscos, os controles internos e conformidade serão integrados ao planejamento estratégico, aos processos e as políticas estabelecidas pelo SERPRO.

5.2 A integração da gestão de riscos ao planejamento estratégico, processos e políticas organizacionais será implementada por meio de aplicação de metodologia específica.

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 5/7          |
| <b>TÍTULO</b><br><b>POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE</b> |        |           |               |        |              |

5.3 A metodologia de gestão de riscos e controles internos, instituída por meio da Decisão de Diretoria RI-115/2016, contempla a sistemática e artefatos utilizados para identificar, avaliar, tratar e monitorar os riscos corporativos.

5.4 A gestão de riscos deve priorizar o tratamento dos processos que concentrem os riscos corporativos críticos. Este tratamento será conduzido pela unidade responsável pela gestão de riscos - Superintendência de Controles, Riscos e *Compliance* - SUPCR, em conjunto com o gestor do processo.

5.5 Para os processos que não concentrem riscos corporativos críticos, o tratamento dos riscos será realizado pelos responsáveis das respectivas unidades organizacionais por meio da auto-aplicação da metodologia.

5.6 Indicadores de riscos e conformidade serão estabelecidos e monitorados respeitando o ciclo dos processos, servindo de base para tomada de decisão quanto aos limites de exposição aos riscos corporativos.

5.7 Planos de capacitação devem estar estruturados, desenvolvidos e aplicados continuamente para todos os empregados e gestores do SERPRO, para fortalecer a cultura organizacional nas áreas de atuação desta política.

5.8 O monitoramento de riscos e conformidade será realizado de forma contínua, permitindo identificar situações adversas e adotar as ações corretivas ou de contorno, minimizando impactos nos processos da organização.

5.9 As eventuais perdas aferidas por meio dos indicadores de monitoramento dos riscos deverão ser consolidadas em mapa de perdas operacionais, para definição de ações e metas de contenção.

5.10 Os relatórios com as ações de tratamento de riscos, as matrizes de exposição a riscos e de perdas serão submetidos semestralmente à Diretoria e ao Conselho Diretor, contemplando o detalhamento dos riscos críticos, dos controles, os responsáveis e prazos para implementação do plano de ações para o tratamento dos riscos.

5.11 O processo de gestão de riscos deve prever mecanismos de comunicação contínua, incluindo relatórios sobre o desempenho da gestão de riscos, como parte do processo de governança.

5.12 A gestão dos riscos relativos a desvios de fraude e corrupção será realizada pelas instâncias intervenientes do Programa de Integridade do Serpro.

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 6/7          |
| TÍTULO  |        |           |               |        |              |
| POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE |        |           |               |        |              |

## 6.0 RESPONSÁVEIS

6.1 O Conselho Diretor é responsável por supervisionar os sistemas de gestão de riscos, controles internos e conformidade.

6.2 A Auditoria Interna é responsável por aferir a efetividade do gerenciamento de riscos e a adequação dos controles internos.

6.3 A Diretoria é responsável por aprovar, cumprir e fazer cumprir a política e normativos relacionados à gestão de riscos, controles internos e conformidade.

6.4 Os Diretores são responsáveis pela execução dos planos de ação de tratamento de riscos das áreas e processos sob sua supervisão.

6.5 A Diretoria de Governança e Gestão -DIGOG é a responsável pela condução das ações de gestão de riscos corporativos.

6.6 A Superintendência de Controles, Riscos e *Compliance* - SUPCR é a unidade organizacional responsável pela gestão e operacionalização desta política no SERPRO.

6.7 O Comitê Estratégico de Governança, Riscos, Controles e Segurança da Informação, instituído pela Decisão de Diretoria OE-123/2016, é o órgão colegiado responsável pela gestão integrada dos riscos operacionais, financeiros e de segurança da informação, bem como supervisionar a institucionalização da gestão de riscos, de controles internos e conformidade, além de propor à Diretoria, limites de exposição a riscos para o SERPRO.

6.8 Comitês Táticos, instituídos por Diretoria, serão voltados ao monitoramento da implementação dos planos de tratamento de riscos das unidades vinculadas.

6.9 Os gestores de processos organizacionais são responsáveis por adotar medidas de gestão de riscos, de controles internos e conformidade, e verificar continuamente sua eficácia, para garantir o alcance dos objetivos empresariais.

6.10 As Unidades são responsáveis pela implementação desta política em seus segmentos de atuação, seguindo as orientações normativas emitidas sobre o tema.

## 7.0 DISPOSIÇÕES FINAIS

7.1 A SUPCR emitirá orientações para adoção e implementação desta política, direcionadas às Unidades do SERPRO.

| ANEXO   | NÚMERO | TIPO DOC. | IDENTIFICAÇÃO | VERSÃO | FOLHA(Nº/DE) |
|---|--------|-----------|---------------|--------|--------------|
|   | 1      | RESOLUÇÃO | RI-020/2016   | -      | 7/7          |
| TÍTULO  |        |           |               |        |              |
| POLÍTICA CORPORATIVA DE GESTÃO DE RISCOS, CONTROLES INTERNOS e CONFORMIDADE |        |           |               |        |              |

7.2 As políticas e documentos organizacionais devem observar e serem ajustados, no que couber, às diretrizes desta política.

7.3 Cabe à SUPCR dirimir dúvidas e coordenar ações para equacionar questões não previstas.

7.4 A não observância desta política e seus desdobramentos normativos implicará, no que couber, em sanções previstas no Regime Disciplinar - Apuração de Responsabilidades e Aplicação de Penalidades e no Código de Ética e de Conduta Empresarial do SERPRO.

7.5 Esta política encontra sua fundamentação na legislação vigente, bem como, no que couber, em padrões, técnicas e conceitos reconhecidamente adotados pelos órgãos de controle:

- a) Instrução Normativa Conjunta CGU e Ministério do Planejamento nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal;
- b) Resoluções da Comissão Interministerial de Governança Corporativa e de Administração de Participações Societárias da União (CGPAR), números 10 a 18, de 10/05/2016;
- c) Lei 12.846/2013, de 01/08/2013, que dispõe sobre a responsabilidade administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública;
- d) Decreto 8.420/2015, de 18/03/2015, que regulamenta a Lei 12.846/2013;
- e) Lei 13.303, de 30/06/2016, que dispõe sobre o estatuto jurídico da empresa pública, da sociedade de economia mista e de suas subsidiárias, no âmbito da União, dos Estados, do Distrito Federal e dos Municípios;
- f) Normas ABNT (Associação Brasileira de Normas Técnicas) ISO 31000:2009, 31010:2012 e GUIA 73:2009;
- g) COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) I e II.