POLÍTICA DE GERENCIAMENTO DE RISCOS DA PROGUARU S.A.

Sumário

Apresentação

A busca dos objetivos de uma organização do setor público envolve riscos decorrentes da natureza de suas atividades, de realidades emergentes, de mudanças nas circunstâncias e nas demandas sociais, da própria dinâmica da administração pública, bem como da necessidade de otimização da transparência e prestação de contas e de cumprir variados requisitos legais e regulatórios.

Assim, as organizações públicas necessitam gerenciar riscos, identificando-os, analisando-os e, em seguida, avaliando se eles devem ser modificados por algum tratamento, de maneira a propiciar segurança razoável para que os objetivos sejam alcançados.

A identificação de riscos permite a determinação de quais riscos podem afetar os programas, projetos ou processos de trabalho. O principal benefício é a documentação dos riscos existentes e a capacidade de se antecipar às ameaças e oportunidades ou diminuir os impactos ocasionados pelo risco.

Nesse sentido, a Proguaru apresenta a sua Política de Gerenciamento de Riscos em plena conformidade com a legislação aplicável e com as normas internacionais que definem conceitos, atribuições e responsabilidades do processo de gestão de riscos, além de orientar a identificação, a análise, a avaliação, o tratamento, o monitoramento e a comunicação dos riscos, com vistas ao alcance dos objetivos institucionais.

Para tanto, a Política apresenta seus objetivos, diretrizes, metodologia e responsabilidades para uma efetiva gestão de riscos. Para a obtenção de sucesso, os conceitos aqui elencados devem ser rigorosamente seguidos, as atividades e os processos devem ser devidamente mapeados e em conformidade com as normativas estabelecidas e, ainda, o mais relevante, todos devem estar envolvidos, atuando com compromisso e comprometimento.

1. Objetivo

O objetivo desta Política é apresentar diretrizes, responsabilidades e metodologia de gerenciamento de riscos da Proguaru, orientando os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos. Assim, pretende-se:

- Ampliar as boas práticas de Governança Corporativa;
- Incorporar a visão de riscos à tomada de decisões estratégicas, em conformidade com as regulamentações aplicáveis e as melhores práticas de mercado;
- Facilitar a identificação de oportunidades e ameaças;
- Realizar uma melhor gestão dos recursos, com base no gerenciamento dos riscos;
- Prezar pela correta aplicação das normativas externas e internas;
- Aperfeiçoar os controles internos das áreas;
- Divulgar a Política de Gerenciamento de Riscos, promovendo uma linguagem comum de gerenciamento de riscos;
- Otimizar a transparência, possibilitando maior controle da sociedade.

2. Termos e Definições

Para fins desta Política, considera-se:

- **Apetite ou propensão ao risco:** grau de exposição aos riscos que a empresa está disposta a aceitar para atingir seus objetivos estratégicos e criar valor para os acionistas.
- **Corrupção:** ação, direta ou indireta, consistente em autorização, oferecimento, promessa, solicitação, aceitação, entrega ou recebimento de vantagem indevida, de natureza econômica ou não, envolvendo agentes públicos ou não, com o objetivo de que pratique ou deixe de praticar determinado ato. A conduta pode ser apenas tentada.
- **Fraude:** qualquer ação ou omissão intencional com o objetivo de lesar ou ludibriar outra pessoa, capaz de resultar em perda para a vítima e/ou vantagem indevida, patrimonial ou não, para o autor ou terceiros. Caracteriza-se também pela declaração falsa ou omissão de circunstâncias materiais com o intuito de levar ou induzir terceiros a erro.
- **Gestão de riscos:** é um meio pelo qual a incerteza é sistematicamente gerenciada para aumentar a probabilidade de cumprir metas e objetivos. O gerenciamento dos riscos visa

avaliar as incertezas que podem prejudicar os objetivos da empresa e executar ações para impedir ou minimizar seu impacto na organização.

- **Identificação do risco:** processo de determinação dos riscos, reconhecimento e descrição das características do risco.
- **Impacto:** efeito resultante da ocorrência de um risco.
- **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 em oportunidade para a empresa.
- **Matriz de riscos:** forma de representação da exposição dos riscos identificados, considerando a avaliação de seu impacto versus sua probabilidade.
- **Probabilidade:** chance de uma incerteza acontecer.
- **Processo:** conjunto ordenado de atividades de trabalho, com início e fim, entradas e saídas bem definidas que são executadas para atingir um objetivo.
- **Proprietário de risco (*Risk Owner*):** o proprietário do risco será aquele que possui autoridade e responsabilidade pelo gerenciamento do risco na empresa. Pode ser aquele que está no setor de trabalho onde um determinado risco é avaliado.
- **Responsável pelo processo (*Process Owner*)**: responsável por determinados processos dentro da companhia. Este colaborador zela pelo ciclo de vida do processo e de seu resultado. Importante ressaltar que *o process owner* é um papel e não um cargo ou função.
- **Resposta ao risco**: é o tratamento que será dado ao risco, tendo como evitar, reduzir, compartilhar ou aceitar o risco.
- **Risco:** evento ou condição de incerteza que, se caso ocorrer, terá um efeito positivo (oportunidade) ou negativo (ameaça).
- **Risco inerente:** risco intrínseco à realização das atividades da empresa.
- **Risco residual:** risco que permanece após a adoção de medidas para a mitigação das avaliações de impacto e probabilidade de materialização dos riscos inerentes.
- **Vulnerabilidade:** o nível de exposição ao risco considerando a atual estrutura de controles da Companhia: técnicas atuais para mitigação de riscos, eficiência e eficácia de controles, histórico e impactos anteriores de riscos, complexidade do gerenciamento de riscos, nível de crescimento e contratação. É a extensão à qual a Companhia pode estar

exposta em relação aos objetivos de negócios ou desprotegida em relação aos impactos negativos depois que os controles existentes foram avaliados.

3. Diretrizes

- A Política de Gerenciamento de Riscos deve considerar a identidade organizacional da Proguaru, considerando missão, visão, valores e objetivos institucionais.
- O Conselho de Administração e a Diretoria devem promover a gestão de riscos em todos os níveis hierárquicos, assegurando a aplicação das diretrizes e a aderência de gerenciamento de riscos.
- O gerenciamento de riscos deve ocorrer em todos os processos de gestão, controles internos e auditoria, assim haverá identificação e gestão tempestiva dos riscos.
- O processo de gerenciamento de riscos deve ter melhoria contínua, os riscos devem ser avaliados e revistos.
- Os riscos identificados devem ser analisados, classificados, priorizados e sua resposta definida, sendo que os proprietários do risco devem realizar planos de ação e contingência, além de monitorá-los.

4. Etapas

As diretrizes apresentadas nesta Política definem e caracterizam as etapas do processo de gestão de riscos. O processo será dividido em 5 etapas, sendo elas:

- *Identificação dos Riscos*: esta etapa consiste em identificar os riscos, descrever os eventos que possam afetar os objetivos. Nesta etapa todos os riscos devem ser identificados para posterior análise;
- *Avaliação e priorização dos riscos*: esta etapa compreende a análise e priorização dos riscos previamente identificados. Eles devem ser classificados em níveis de criticidade (Muito Alta, Alta, Média, Baixa e Muito Baixa);
- *Tratamento e resposta aos riscos:* esta etapa consiste em desenvolver alternativas, selecionar estratégias e acordar ações para lidar com a exposição geral aos riscos, e tratar os riscos individuais previamente priorizados;

- *Monitoramento e controle dos riscos*: esta etapa consiste em monitorar a implementação de planos acordados de resposta aos riscos, acompanhamento de riscos identificados, identificação e análise de novos riscos e avaliação da eficácia do gerenciamento do risco ao longo do tempo.
- *Comunicação e revisão dos riscos*: esta etapa propõe ações corretivas e registra as lições aprendidas. Também serve para reavaliar e alterar a priorização de riscos previamente identificados.

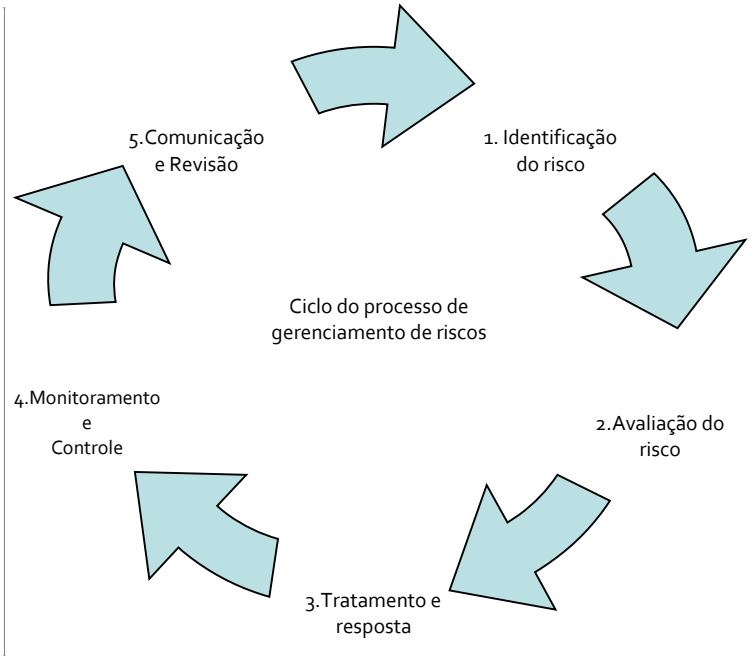

Figura 1 - Ciclo do processo de gestão de risco

4.1. Identificação dos riscos

Um dos papéis do gerenciamento de riscos é mapear todos os fatores prejudiciais antes mesmo que eles aconteçam. Para isso, é necessário o desenvolvimento de ações que possam prever tais eventos. A administração avalia os eventos com base em duas perspectivas – probabilidade e impacto – e, geralmente, utiliza uma combinação de métodos qualitativos e quantitativos. Os impactos positivos e negativos dos eventos em potencial devem ser analisados isoladamente ou por categoria em toda a organização. Os riscos são avaliados com base em suas características inerentes e residuais.

Dentre os objetivos do Mapa de Riscos estão:

- Reunir informações suficientes para estabelecer um diagnóstico da situação de risco;
- Possibilitar a troca e divulgação de informações entre os colaboradores, bem como estimular sua participação nas atividades de prevenção;
- Reconhecer e descrever os riscos aos quais a empresa está exposta.

A identificação dos riscos deve ser realizada com a participação de todos os envolvidos nos processos de negócio da empresa, nos seus diferentes níveis. Nesta etapa os riscos devem ser classificados e registrados em sistema adequado.

Os riscos devem ser classificados como:

1. Riscos Estratégicos: é a probabilidade de o ambiente externo à organização provocar situações ou quando do não planejamento estratégico adequado, que impedem o crescimento da organização;

2. Riscos Operacionais: eventos que podem comprometer as atividades da empresa associados a falhas, deficiências ou inadequações de processos internos, pessoas, infraestrutura e sistemas, afetando o esforço da gestão;

3. Riscos Financeiros: eventos que podem comprometer a capacidade da Proguaru SA de contar com os recursos orçamentários necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária, como atrasos no cronograma de pagamentos;

4. Risco Reputacional: eventos que podem comprometer a confiança da sociedade em relação a capacidade da Proguaru SA em cumprir sua missão institucional que interferem diretamente na imagem da empresa;

5. Riscos de Conformidade: eventos que podem afetar o cumprimento de leis, diretrizes, normas e regulamentos aplicáveis;

6. Riscos de Integridade: riscos que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

O processo de identificação de riscos deve ocorrer ao longo da vida do objeto da gestão, pois antigos riscos podem ser eliminados e novos poderão surgir.

4.2. Avaliação dos riscos

Após a identificação dos riscos, devem ser realizadas análises qualitativas e/ou quantitativas, visando à definição dos atributos de impacto e probabilidade, utilizados na priorização dos riscos a serem tratados. A avaliação de riscos deve considerar, inclusive, o levantamento e a análise dos controles e indicadores que serão criados.

Nesta etapa a empresa deverá aplicar algumas ferramentas para melhor visualização e classificação dos riscos.

A seguir, algumas das principais ferramentas para gerenciamento de riscos:

- Matriz de Probabilidade e Impacto (Matriz PI):

A matriz de probabilidade e impacto serve para categorizar e priorizar riscos de modo que os mais graves sejam gerenciados primeiro. A primeira análise a ser efetuada é a de probabilidade. Utilizando uma escala de 1 a 5 determina-se qual a probabilidade de uma incerteza ocorrer, conforme descrito na tabela abaixo:

Descritor	Descrição	Nível
Muito baixo	Probabilidade muito pequena de ocorrer, nunca ocorreu antes	1
Baixo	Probabilidade baixa de ocorrer, já ocorreu pouquíssimas vezes	2
Médio	Probabilidade significante de ocorrer, já ocorreu outras vezes	3
Alto	Probabilidade muito significante de ocorrer, já ocorreu diversas vezes antes	4
Muito Alto	Certamente irá ocorrer	5

Tabela 1 – Probabilidade de eventos

A segunda análise a ser realizada é a de impacto da ocorrência dos eventos. Utilizando uma escala de 1 a 5 determina-se qual o impacto que a incerteza irá gerar caso ele ocorra, conforme proposto a seguir:

Descritor	Descrição	Nível
Muito baixo	Impacto INSIGNIFICANTE nos objetivos da empresa	1
Baixo	Impacto MÍNIMO nos objetivos da empresa	2
Médio	Impacto MEDIANO nos objetivos da empresa, com possibilidade de recuperação	3
Alto	Impacto SIGNIFICANTE nos objetivos da empresa, com remota possibilidade de recuperação	4
Muito Alto	Impacto MÁXIMO nos objetivos da empresa, SEM possibilidade de recuperação	5

Tabela 2 – Impacto da ocorrência de eventos

- Análise Probabilidade x Impacto:

Este é o processo de analisar numericamente os efeitos dos riscos nos objetivos gerais. Considera-se, por meio de análises, a exposição que a organização tem aos riscos identificados. Baseado na análise realizada anteriormente, deve-se realizar a multiplicação simples dos valores de probabilidade e impacto e, após, atribuir o valor a cada risco previamente identificado, conforme o exemplo a seguir:

Cód.	Severidade	Descrição do risco	Probabilidade	Impacto
1	6	Aplicação de multa por falta de licenças de software	3-Média	2-Baixo
2	4	Multa da TCE por não importação de informações de contrao para sistema da Audesp	1-Muito baixa	4-Alto
3	20	Parada de sistemas críticos	4-Alta	5-Muito Alto
4	9	Quebra de confidencialidade de informações sensiveis nos servidores	3-Média	3-Médio
5	5	Queda de aeronave na sala de servidores	1-Muito baixa	5-Muito Alto
6	20	Interrupção no fornecimento dos links de internet	5-Muito Alta	4-Alto

Tabela 3 - Classificação de severidade

- Matriz de Risco (Heat Map):

Matriz de Risco apresenta nos seus eixos escalas de probabilidade de ocorrência e impacto corporativo para um dado fator de risco. Desenhada a estrutura da matriz, cada um dos fatores de risco identificado (a identificação dos fatores de risco é a primeira etapa de um sistema de Gerenciamento do Risco Corporativo) deve ser avaliado (qualitativamente, a priori) em termos de probabilidade e impacto, e posicionado na Matriz de Risco. A região vermelha engloba os riscos que devem ser tratados prioritariamente:

PROBABILIDADE \ IMPACTO	Muito Baixo	Baixo	Médio	Alto	Muito Alto
Muito Alto	Significante	Pouco Crítico	Crítico	Muito Crítico	Muito Crítico
Alto	Significante	Muito Significante	Pouco Crítico	Crítico	Muito Crítico
Médio	Pouco Significante	Significante	Muito Significante	Pouco Crítico	Crítico
Raro	Insignificante	Pouco Significante	Significante	Muito Significante	Pouco Crítico
Muito Raro	Insignificante	Insignificante	Pouco Significante	Significante	Muito Significante

Tabela 4 – Heat Map

- Análise e Priorização dos riscos:

Este é o processo de priorização dos riscos para análise ou ação adicional através da avaliação e combinação de sua probabilidade de ocorrência e impacto. Neste processo, faremos uma análise subjetiva com o propósito de priorizar riscos a partir da probabilidade de impacto medida durante a análise dos riscos e, também, determinar o que precisa ser acompanhado durante o período de vida do risco e o que deve ficar em quarentena.

Severidad	Descrição do risco	Probabilidad	Impacto	Descrição do Impacto	Categoria	Tipo
25	Multa da TCE por não importação de informações de contrato para sistema da	5-Muito Alta	5-Muito Alto	Aplicaçao de TAC por não cumprimento de prazo 90 dias estipulado pelo TCE.	Legal	Externo
20	Parada de sistemas críticos	4-Alta	5-Muito Alto	Queima de servidor, perda de dados, paralisaçao da empresa.	Operacional	Interno
20	Quebra de confidencialidade de informações sensiveis nos servidores	4-Alta	5-Muito Alto	Invasão hacker, alteraçao funcionarios setor.	Operacional	Interno
20	Perda de Prazos legais por queda de energia na sala de servidores	4-Alta	5-Muito Alto	A queda de energia repentina pode danificar servidores acarretando a impossibilidade de execucao de serviços ou perda de dados que impossibilite trabalhos com data de entrega	Legal	Externo
20	Perda de dados criticos por invasão de hacker	4-Alta	5-Muito Alto	A vulnerabilidade da empresa em sua rede e quebra da confidencialidade pela	Operacional	Externo
16	Perda de dados criticos por queda de energia	4-Alta	4-Alto	A queda de energia repentina pode danificar servidores acarretando a impossibilidade de execucao de serviços ou perda de dados que impossibilite trabalhos com data de entrega	Operacional	Interno

Tabela 5 - Priorização de riscos

4.3 Resposta e tratamento dos riscos

Posteriormente à avaliação, deve-se definir o tratamento que será dado aos riscos priorizados e como esses deverão ser monitorados e reportados às diversas partes envolvidas.

Tratar os riscos consiste em decidir entre:

- Eliminar;
- Mitigar, pela definição de planos de ação e controles internos;
- Transferir; ou
- Aceitar.

A decisão sobre a estratégia adotada para tratar cada risco depende principalmente do grau de apetite ao risco da empresa, previamente homologado pelo seu Conselho de Administração.

- Plano de resposta aos riscos:

Planejar a resposta aos riscos tem como objetivo desenvolver opções e ações para aumentar as oportunidades e reduzir as ameaças aos objetivos da organização.

Trata a resposta aos riscos conforme sua prioridade e define um "proprietário" para cada risco.

A resposta tratada deve implicar em mais recursos e atividades no orçamento e cronograma da organização.

Cód.	Severidade	Descrição do risco	Probabilidade	Impacto	Descrição do Impacto	Categoria	Ação	Descrição da ação	Responsável	Previsão Gasto
1	12	Perda de dados da empresa por exclusão acidental por parte de colaboradores	4-Alta	3-Médio	Funcionários podem acidentalmente apagar dados importantes.	Organizacional	Mitigar	Aquisição de discos para backup de dados e treinamento para colaboradores da empresa	Marcelo Brito - TI	R$23.534,81
2	15	Ataque de hackers, infestação por vírus ou sequestro digital	3-Média	5-Muito Alto	Empresa pode ficar sem ferramentas digitais para executar suas atividades	Externo	Transferir	Contratar consultoria de Segurança, instalar antivirus e firewall de borda na rede Proguaru	Marcelo Brito - TI	R$112.532,51

Tabela 6 - Plano de resposta aos riscos

- **Eliminar**: Alterar o plano do projeto para eliminar totalmente o risco, protegendo os objetivos do projeto dos impactos deste risco eliminado.;
- **Mitigar**: Reduzir a probabilidade ou impacto de um risco até um nível aceitável;
- **Transferir**: Transferir o risco para um terceiro, transferindo os impactos e a responsabilidade. É preciso ter em mente que o risco não é eliminado, e quase sempre envolve o pagamento de prêmios à parte que está assumindo o risco;
- **Aceitar**: Quando não é possível aplicar nenhuma das outras estratégias, a equipe do projeto decide correr o risco.

4.4 Monitoramento dos riscos

No processo de monitoramento, deve-se supervisionar a implantação e manutenção dos planos de ação; verificar o alcance das metas das ações estabelecidas, através de atividades gerenciais contínuas e/ou avaliações independentes; garantir que os controles sejam eficazes e eficientes; detectar mudanças no contexto externo e interno, identificando riscos

emergentes; e analisar as mudanças nos eventos de risco, tendências, sucessos e fracassos e aprender com eles.

Esta etapa também inclui tomar as medidas de correção que se mostrarem necessárias na revisão do plano, atualizar os registros e documentos gerados, garantir que a gestão de riscos esteja sendo efetiva.

O monitoramento deve ser realizado de forma contínua, pelos responsáveis das atividades e pelos seus respectivos gestores

- Indicadores (Risco, Probabilidade e Impacto):

Indicadores são os parâmetros de acompanhamento e comparação para análise e eventual tomada de decisão sobre os principais riscos aos quais uma empresa está exposta. São eles os responsáveis por medirem os riscos potenciais e por permitirem ações em tempo hábil, garantindo, desse modo, o sucesso de uma organização.

Com os Indicadores as empresas estão aptas a:

- Destacar os pontos fracos de controle e permitir o fortalecimento de controles deficientes;
- Facilitar o processo de notificação e escalonamento de riscos;
- Fornecer informações detalhadas aos gestores sobre estratégias a serem tomadas para evitar um risco;
- Cumprir os requisitos regulamentares;
- Incentivar seu quadro de colaboradores sobre a importância da Gestão de Riscos;
- Promover a conscientização das questões envolvendo os riscos de quaisquer atividades da empresa;
- Reportar os níveis de risco o mais rapidamente possível;
- Garantir controles efetivos;
- Entender como o perfil do risco muda em diferentes circunstâncias;
- Entender os sinais de possíveis riscos que podem vir a afetar a empresa;
- Detectar problemas como parte de um “sistema de alerta precoce”, o que permite a empresa a definir os riscos, preveni-los e mitigá-los.

4.5 Comunicação e revisão dos riscos

A comunicação durante todas as etapas do processo de gestão de riscos deve atingir todas as partes interessadas, sendo realizada de maneira clara e objetiva, respeitando as boas práticas de governança exigidas pelo mercado.

O comitê de riscos deverá realizar reuniões periódicas com as áreas gestoras do risco, em que serão discutidos e verificados os riscos classificados. Nessa reunião novos riscos identificados deverão ser apontados.

Os proprietários do risco deverão definir os planos de tratamento para os riscos sob sua responsabilidade e submetê-los ao comitê de riscos para análise e posterior aprovação da diretoria.

5. Responsabilidades – Partes interessadas

- **Áreas proprietárias de riscos** – atuar como primeira linha de defesa da empresa, gerenciando os riscos inerentes às suas atividades, identificando-os, avaliando-os e tratando-os de modo a otimizar suas decisões, com o intuito de manter e obter vantagens competitivas e garantir a geração de valor para acionistas e demais partes interessadas.

- **Conselho de Administração** – deliberar sobre as questões estratégicas concernentes ao processo de gestão de risco, tais como o grau de apetite a riscos da empresa, o papel das diretorias executivas no gerenciamento dos riscos e a política que deve nortear todo o processo;

- **Comitê de Auditoria Estatutário** – assessorar, na qualidade de órgão consultivo, o Conselho de Administração no cumprimento das responsabilidades de fixação de diretrizes fundamentais e de controle superior da empresa, com atribuições específicas de análise, acompanhamento e recomendação sobre questões relacionadas ao controle interno e à gestão de riscos, em particular acompanhando os riscos de negócio da PROGUARU e recomendando ações de mitigação;

- **Comitê de risco** – coordenar e definir os padrões a serem seguidos, no que tange aos processos de gestão de riscos, aos seus sistemas de suporte e às formas e à periodicidade de seus reportes; apoiar e garantir a identificação e o monitoramento dos riscos pelas áreas proprietárias, de acordo com as políticas e técnicas aprovadas pelas diretorias executivas da empresa;

- **Diretorias executivas** – patrocinar a implantação da gestão de riscos na PROGUARU; alocar recursos necessários ao processo e definir a infraestrutura apropriada às atividades de gerenciamento de riscos; aprovar normas específicas; deliberar sobre decisões estratégicas considerando as análises dos riscos relatadas pelo comitê de riscos;

- **Gerência de Controle Interno** – efetivar as ações necessárias ao estabelecimento do ambiente de controles para auxílio no tratamento e monitoramento dos riscos identificados pelas áreas proprietárias, além de realizar a consolidação do ambiente de controles internos da PROGUARU, a partir de informações recebidas de áreas equivalentes.

6. Revisão e atualização da Política de Gerenciamento de Riscos

O comitê de riscos deverá realizar uma reunião anual a fim de revisar a política de gerenciamento de riscos; avaliar se houve mudanças no processo e sugerir ações corretivas e relatar as lições aprendidas. Para tal, serão considerados, entre outros itens, comentários e sugestões recebidas dos colaboradores, diretores e conselheiros, as alterações na lei ou práticas recomendadas, bem como a experiência adquirida na aplicação da Política.

As alterações realizadas na Política serão prontamente divulgadas e disponibilizadas no Portal de Transparência da Proguaru.

7. Disposições Gerais

- Esta política deve ser acompanhada pelo Conselho de Administração e diretorias executivas da PROGUARU, no que tange à aplicação dos procedimentos de acompanhamento e ao controle de suas diretrizes.

- A PROGUARU deve garantir que os princípios e diretrizes estabelecidos nesta Política sejam seguidos e observados.

- O presente documento deve ser lido e considerado em conjunto com outros padrões, normas e procedimentos aplicáveis e relevantes, adotados pela PROGUARU, em particular aqueles relacionados a fraudes, corrupção e conduta antiética. Além disso, considerando as especificidades de cada departamento, esta Política deve ser desdobrada em outros documentos normativos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

- As exceções, eventuais violações e casos omissos a esta Política devem ser submetidos à apreciação do Comitê de Riscos da PROGUARU e encaminhados para posterior aprovação.

8. Bibliografia

Bernstein, P. *Desafio aos Deuses: A Fascinante História do Risco*. 3. ed. Campus, Rio de Janeiro, 1996.

Brealey, R. & Myers, S. *Financiamento e Gestão de Risco*. Porto Alegre, Bookman, 2005.

Brigham, E. F.; Gapenski, L. C. & Ehrardt, M. C. *Administração Financeira: Teoria e Prática*. São Paulo, Atlas, 2001.

Burnaby, Priscilla & Hass, Susan. "Ten Steps to Enterprise-wide Risk Management". *Corporate Governance*, vol 9, n. 5, 2009.

Coso. *Gerenciamento de Riscos Corporativos – Estrutura Integrada – Sumário Executivo Estrutura*. PriceWaterhouseCoopers,
São Paulo, 2007.

COSO 2013 (Committee of Sponsoring Organizations of the Treadway Commission) – Internal Control – Integrated Framework;

COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission) – Enterprise Risk Manangement Framework;

Crouhy M.; Galai, D. & Mark, R. *Gerenciamento de Risco: Abordagem Conceitual e Prática – Uma Visão Integrada*
dos Riscos de Crédito e de Mercado. Rio de Janeiro/São Paulo, Qualitymark/Serasa, 2004.

Doherty, Neil A. *Integrated Risk Management: Techniques and Strategies for Managing Corporate Risk*. Nova York,
McGraw-Hill, 2000.

Faber, M.; Manstetten, R. & Proops, J. *Ecological Economics: Concepts and Methods*. Cheltenham, Edward Elgar
Publishing Ltd., 1996.

Galesne, A; Fensterseifer, J. E. & Lamb, R. *Decisões de Investimentos da Empresa*. São Paulo, Atlas, 1999.

Gerenciamento de Riscos Empresariais. 2. ed. revista e ampliada. Rio de Janeiro, Elsevier (Editora Campus), 2005.

Grinblat, M. & Titman, S. *Mercados Financeiros e Estratégia Corporativa*. Porto Alegre, Bookman, 2005.

IBGC (Instituto Brasileiro de Governança Corporativa). *Código das Melhores Práticas de Governança Corporativa*.

Instrução Normativa Conjunta MPOG/CGU no 1, de 10/05/2016

Jorion, P. *Value-at-Risk: A Nova Fonte de Referência para a Gestão do Risco Financeiro*. São Paulo, BM&F, 2003.

Kaplan, Robert S. & Mikes, A. "Gestão de Riscos: Um Novo Modelo". *Harvard Business Review*, jun. 2012.

NACD (National Association of Corporate Directors). *Report of the NACD Blue Ribbon Commission on Risk*
Governance: Balancing Risk and Reward. Washington (DC), NACD, 2009.

Norma ABNT NBR ISO 31000:2009 – Gestão de Riscos: Princípios e Diretrizes;

Norma ABNT ISO GUIA 73:2009 – Gestão de Riscos: Vocabulário.

Norma ABNT (Associação Brasileira de Normas Técnicas). NBR ISO 31.000: 2009, Gestão de Riscos – Princípios e Diretrizes.

Ross, S. A.; Westerfield, R. W.; Jaff e, J. & Lamb, R. *Administração Financeira*. Porto Alegre, Grupo AMGH, 2015.

Sarbanes-Oxley Act. Public Company Accounting Reform and Investor Protection Act of 2002, EUA, 2002.

Scott, H. *Risk Management and Insurance*. 2. ed. Boston, Mc Graw Hill, 2010.

Vaughan, E. J. & Elliot, C. M. *Fundamentals of Risk and Insurance*. 9. ed. Nova York, Wiley, 2003.

Anbima *Perspectivas: A Reforma Financeira Norte-Americana – A Lei Dodd/Frank*. *Disponível em:* http://www.anbima.com.br/data/files/B2/24/B5/51/742D7510E7FCF875262C16A8/Perspectivas_20ANBIMA_20Reforma_20Americana_1_.pdf
Acesso em: 15 dez. 2016.

Baraldi, Paulo A. “Apetite e Tolerância aos Riscos”. 2013.
Disponível em: www.riskatrisk.com.br/APETITE_E_TOLERANCIA_AOS_RISCOS1.pdf
Acesso em: 9 dez. 2016.

Como Alinhar Estratégias a Objetivos e Metas e ao Processo de Decisão”. 2013.
Disponível em: <www.riskatrisk.com.br/imagens-para-site/Alinhar.Estratégias.Metas.pdf>.
Acesso em: 9 dez. 2016.

Código de Conduta do IBGC. São Paulo, IBGC, 2013.
Disponível em: http://www.ibgc.org.br/index.php/publicacoescodigo-de-conduta
Acesso em: 9 dez. 2016.

Código das Melhores Práticas 5. ed. São Paulo, 2015.
Disponível em: http://www.ibgc.org.br/index.php/publicacoes/codigo-dasmelhores-praticas
Acesso em: 9 dez. 2016.

Declaração de Posicionamento do IIA: As Três Linhas de Defesa no Gerenciamento Eficaz de Riscos e Controles. Jan. 2013. *Disponível em:* http://www.iiabrasil.org.br/new/2013/downs/As_tres_linhas_de_defesa_Declaracao_de_Posicionamento2_opt.pdf
Acesso em: 12 set. 2016.

Guia de Orientação para Gerenciamento de Riscos Corporativos. São Paulo, IBGC, 2007
Disponível em: <http://www.ibgc.org.br/index.php/publicacoescadernosde-governanca
Acesso em: 9 dez. 2016.

Gestão Integrada de Riscos: Banco Real e Brasil Telecom. São Paulo, IBGC, 2008
Disponível em: http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos
Acesso em: 9 dez. 2016.

Gestão de Riscos como Instrumento para a Tomada de Decisão: Votorantim Celulose e Papel (VCP). São
Paulo, IBGC, 2008
Disponível em: http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos
Acesso em: 9 dez. 2016.

Visão Evolutiva do Modelo de Gestão de Riscos: Vale e Natura Cosméticos. São Paulo, IBGC, 2008
Disponível em: http://www.ibgc.org.br/index.php/publicacoes/estudos-de-casos
Acesso em: 9 dez. 2016.

ANEXO – FLUXOGRAMA DE GERENCIAMENTO DE RISCOS