Política de Gerenciamento de Risco Operacional

Abril de 2023

Elaboração: Risco

Aprovação: Diretoria Executiva

Classificação do Documento: Público

ÍNDICE

1. INTRODUÇÃO 3
2. OBJETIVO 3
3. ABRANGÊNCIA 3
4. DEFINIÇÕES 3
   4.1. Risco Operacional 3
   4.2. Evento de Risco Operacional 3
   4.3. Causas de Risco Operacional 4
5. ESTRATÉGIA 4
6. ESTRUTURA DE GERENCIAMENTO DE RISCO OPERACIONAL 5
7. RESPONSABILIDADES 7
   7.1. Da Diretoria Executiva 7
   7.2. Do Comitê de Risco 7
   7.3. Do Comitê de Segurança da Informação 8
   7.4. Do Chief Risk Officer (“CRO”) 8
   7.5. Da Área de Auditoria Interna 8
   7.6. Da Unidade de Gerenciamento de Riscos 8
   7.7. Da Área de Controles Internos 9
   7.8. Da Área de Compliance 9
   7.9. Da Área de Segurança da Informação 10
   7.10. Dos Gestores e Colaboradores 10
   7.11. Do Jurídico 11
8. DIRETRIZES DE GERENCIAMENTO DE RISCO OPERACIONAL 11
9. METODOLOGIA 11
   9.1. Identificação 11
   9.2. Avaliação e Mensuração 12
   9.3. Controle 14
   9.4. Monitoramento e Reporte 14
10. REVISÃO E APROVAÇÃO 14

1. INTRODUÇÃO

O gerenciamento de risco operacional permite identificar, avaliar e administrar riscos diante de incertezas além de integrar o processo de criação e preservação de valor para as instituições pertencentes ao Conglomerado Prudencial Genial ("o Conglomerado Genial"). O processo é conduzido pela Diretoria Executiva e pelos demais colaboradores e é aplicado no estabelecimento de estratégias, de forma compatível com o apetite a risco, possibilitando um nível razoável de garantia em relação à realização de seus objetivos.

2. OBJETIVO

Esta Política tem por objetivo estabelecer os fundamentos associados ao processo de gerenciamento integrado de risco operacional em conformidade com a Resolução CMN 4.557, de 23 de fevereiro de 2017.

3. ABRANGÊNCIA

Estão sujeitas às regras e premissas definidas nesta política: (i) Todas as empresas e instituições pertencentes ao Conglomerado Genial e suas controladas; (ii) Todos os colaboradores e, (iii) Qualquer empresa prestadora de serviços e/ou funcionários terceirizados.

4. DEFINIÇÕES

Os principais termos contidos nesta política corporativa envolvem as seguintes definições:

4.1. Risco Operacional

Para efeitos desta política, define-se o risco operacional como a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. O risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, bem como as sanções em razão de descumprimento de dispositivos legais e as indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição também são consideradas.

4.2. Evento de Risco Operacional

Define-se como evento de risco operacional o incidente relativo à materialização do risco operacional que causa impacto negativo na instituição. Entre os eventos de risco operacional, incluem-se:

- Fraudes internas;
- Fraudes externas;
- Demandas trabalhistas e segurança deficiente do local de trabalho;
- Práticas inadequadas relativas a clientes, produtos e serviços;
- Danos a ativos físicos próprios ou em uso pela instituição;
- Eventos que acarretem na interrupção das atividades da instituição;
- Falhas em sistemas de tecnologia da informação;
- Falhas na execução, cumprimento de prazos e gerenciamento das atividades da instituição.

4.3. Causas de Risco Operacional

As causas são ações ou um conjunto de circunstâncias que levam à ocorrência de um evento de risco operacional, normalmente relacionada à deficiência ou ausência de controles adequados. Podem ser segregadas em quatro fatores de risco:

- Pessoas: Ações humanas intencionais ou não (erros humanos) que podem causar distintos eventos de risco operacional ou problemas decorrentes da falta de recursos humanos (seja na quantidade ou na capacidade técnica).
- Processos: Deriva da interrupção, falha ou falta de controle, desenho inadequado de processos dentro das linhas de negócio ou em processos de apoio.
- Sistemas: Deficiências decorrentes do desempenho dos sistemas; Sistemas não adequados, sistemas obsoletos, falhas com a comunicação externa, alterações efetuadas em sistemas (rotinas) que incorrem em eventos em áreas distintas a área de Tecnologia. Este fator de risco considera a interrupção de comunicação para terceiros.
- Fatores externos: Este fator de risco é oriundo de ocorrências externas que impactam negativamente nas entidades pertencentes ao Conglomerado e relacionam-se com a deficiência decorrente da incapacidade ou ineficiência em tratar tais ocorrências.

5. ESTRATÉGIA

A estratégia definida pela Diretoria é que a Genial utilize as melhores práticas para atuar de forma preventiva mantendo um *framework* robusto e proporcional à dimensão e a relevância das respectivas exposições para mitigar o risco operacional e os efeitos agregados dos demais riscos que podem afetar a realização dos objetivos da Instituição.

6. ESTRUTURA DE GERENCIAMENTO DE RISCO OPERACIONAL

A estrutura de gerenciamento de risco operacional adotada deve ser compatível com o modelo de negócio, com a natureza das operações e com a complexidade dos produtos e serviços, das atividades e dos processos. A estrutura contém mecanismos que permitam a implementação e a disseminação da cultura de risco operacional, das políticas, dos processos e de infraestrutura condizentes com as entidades pertencentes a Genial. Assegurar a aderência e comprometimento de todos os colaboradores para a adequada gestão do risco operacional, Continuidade de Negócios e dos objetivos da Instituição.

O envolvimento da Alta Administração e principais gestores é contínuo e se dá na condução do dia a dia e nos comitês de gestão e controle, notadamente a Diretoria Executiva, Comitê de Risco, Comitê de Segurança, Comitê de Produtos, Comitê de Compliance e Prevenção de Lavagem de Dinheiro, Comitê de Crédito, Comitê de ESG, Comitê de Remuneração e Comitê de Auditoria Interna. Os comitês possuem por função primordial manter o sistema de gerenciamento de risco alinhado com as melhores práticas de Governança.

Desta forma, a instituição demonstra um ambiente interno propício para a prática de controles internos e gestão de riscos onde os objetivos estratégicos são fixados, os eventos de risco identificados e avaliados e uma resposta para a ocorrência dos riscos mapeados é estabelecida. A Genial possui atividades de controle, um fluxo de informações e comunicações e, por fim, um monitoramento contínuo dos riscos relevantes.

Com o intuito de mitigar de forma eficiente os riscos incorridos pela instituição, a Genial e suas controladas atuam utilizando as melhores práticas de mercado, gerenciando os riscos através de Três Linhas de Defesa. Este modelo é uma forma simples e eficaz de melhorar a comunicação do gerenciamento de riscos por meio do esclarecimento dos papéis e responsabilidades essenciais dentro da instituição, conforme diagrama abaixo:

1ª LINHA DE DEFESA: Como primeira linha de defesa, todos os funcionários devem gerenciar os riscos inerentes as suas atividades do dia-a-dia. Todos são responsáveis por identificar, avaliar, controlar, mitigar os riscos encontrados, sugerir e, quando aplicável, implementar as ações corretivas para resolver deficiências em processos e controles relacionados as suas rotinas. Por meio de uma estrutura de responsabilidades em cascata, todos os gerentes devem desenvolver e implementar procedimentos detalhados de controle e supervisão das rotinas executadas por sua equipe, guiando o desenvolvimento e a implementação das políticas e procedimentos internos, garantindo que as atividades estejam de acordo com as metas e objetivos traçados pela instituição.

2ª LINHA DE DEFESA: No mundo ideal, talvez, apenas uma linha de defesa fosse o suficiente para garantir o gerenciamento eficaz dos riscos e controles de conformidade. No mundo real, no entanto, uma única linha de defesa pode, muitas vezes, se provar inadequada. A Diretoria Executiva estabeleceu diversas funções de gerenciamento de riscos e conformidade para ajudar a desenvolver e/ou monitorar os controles da primeira linha de defesa.

As funções da segunda linha de defesa incluem:

- Estabelecer de rotinas e comitês que visem facilitar e monitorar a implementação de práticas eficazes de gerenciamento de riscos e conformidade por parte da 1ª Linha de defesa;
- Auxiliar na definição de apetite de risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente asinformações relacionadas ao tema em todas as linhas de negócio;
- Monitorar riscos específicos, como, por exemplo, a não conformidade com leis e regulamentos aplicáveis a instituição. Nesse caso, o Compliance é a área responsável e reportará eventuais inconsistências diretamente a Diretoria Executiva;
- Orientar sobre processos de gerenciamento de riscos e conformidade;
- Identificar mudanças no cenário regulatório e de riscos, e alertar a 1ª Linha de Defesa de tais inovações.

Cada uma das áreas apresentadas na 2ª linha de defesa guarda um certo nível de independência em relação à 1ª linha de defesa e são, por natureza, funções de gestão. Como funções de gestão, elas podem intervir diretamente, sugerindo a alteração de procedimentos e o desenvolvimento de sistemas de controles internos à 1ª linha de defesa.

3ª LINHA DE DEFESA: A Auditoria Interna é a área com maior nível de independência e objetividade dentro da instituição, reportando-se diretamente a Diretoria Executiva. A auditoria interna realiza avaliações sobre a eficácia da governança, do gerenciamento de riscos e dos controles internos realizados pela 1ª e 2ª linhas de defesa. O resultado dessas avalições é encaminhado periodicamente à Diretoria Executiva.

7. RESPONSABILIDADES

Em linha com o escopo desta política, seguem abaixo as responsabilidades dos envolvidos nos principais processos de gerenciamento de riscos:

7.1. Da Diretoria Executiva

- Aprovar com periodicidade mínima anual as políticas, estratégias e limites para o gerenciamento de risco operacional, bem como o programa de testes de estresse e as políticas para gestão de continuidade de negócios;
- Definir os níveis de apetite por riscos que as entidades pertencentes ao Conglomerado Genial devem aceitar e revisá-los com periodicidade mínima anual, com auxílio do Comitê de Risco e do CRO;
- Manifestar-se sobre as ações incluídas nos relatórios Controles Internos, bem como fazer constar nos relatórios, sua responsabilidade sobre as informações divulgadas;
- Assegurar a aderência da instituição às políticas, estratégias e limites de gerenciamento de riscos;
- Garantir que a estrutura de remuneração da instituição não incentive comportamentos incompatíveis com os níveis de apetite a risco dispostos na RAS;
- Assegurar a correção tempestiva das deficiências da estrutura de gerenciamento de riscos;
- Promover a disseminação da cultura de gerenciamento de riscos na instituição;
- Autorizar, quando necessário, exceções à política, aos procedimentos, aos limites e aos níveis de apetite por riscos fixados na RAS;
- Assegurar recursos adequados e suficientes para o exercício das atividades de gerenciamento de riscos, de forma independente, objetiva e efetiva;
- Indicar o diretor responsável pela Unidade de Gerenciamento de Riscos.

7.2. Do Comitê de Risco

- Revisar a política de gerenciamento de risco operacional anualmente;
- Compreender, de forma abrangente e integrada, os riscos que podem impactar o capital e a liquidez;
- Assessorar a Alta Administração no desempenho de suas atribuições relacionadas à adoção de estratégias, políticas e medidas voltadas à disseminação da cultura, mitigação de riscos e da conformidade com as normas aplicáveis;
- Estabelecer diretrizes para garantir o cumprimento à regulamentação vigente, inibir riscos incompatíveis e/ou desnecessários às entidades pertencentes ao Conglomerado Genial, aumentar a eficácia das áreas de negócios, melhorar a efetividade dos controles e minimizar o impacto aos riscos a que estão sujeitos.

7.3. Do Comitê de Segurança da Informação

- Revisar as políticas e diretrizes de segurança da informação e cibernética;
- Avaliar os diversos tipos de riscos relacionados à Segurança Cibernética e continuidade de negocios e deliberar sobre as ações de mitigação apresentadas.

7.4. Do Chief Risk Officer ("CRO")

- Supervisionar o desenvolvimento, implementação e desempenho da estrutura de gerenciamento de risco operacional, incluindo seu aperfeiçoamento;
- Avaliar e garantir a adequação, à RAS e aos objetivos estratégicos da instituição, da política, dos processos, dos relatórios, dos sistemas e dos modelos utilizados no gerenciamento de risco de operacional;
- Capacitar adequadamente os integrantes da Unidade de Gerenciamento de Riscos acerca da política, dos processos, dos relatórios, dos sistemas e dos modelos da estrutura de gerenciamento de riscos, mesmo que desenvolvidos por terceiros;
- Subsidiar e participar no processo de tomada de decisões estratégicas relacionadas ao gerenciamento de risco operacional, auxiliando a Diretoria Executiva.
- Indicar as diretrizes a serem seguidas no programa de testes de estresse.

7.5. Da Área de Auditoria Interna

- Avaliar periodicamente os processos e procedimentos relativos ao gerenciamento de riscos;
- Identificar, analisar e documentar os riscos relevantes para o atendimento aos objetivos de negócio da Organização;
- Desenvolver um plano de auditoria anual baseado em risco e um planejamento cíclico de longo prazo com possibilidade de ajustes ao longo do tempo em caso de necessidade;
- Avaliar a adequação dos controles estabelecidos para assegurar conformidade com as políticas, procedimentos, leis, regras e objetivo do negócio;
- Avaliar os métodos de salvaguardas de ativos da organização e seus clientes;
- Avaliar a confiabilidade e segurança das informações financeiras e gerenciais, além dos sistemas e operações que geram esses dados;
- Acompanhar ("follow - up") os pontos identificados para assegurar o cumprimento das ações recomendadas, no prazo estabelecido.

7.6. Da Unidade de Gerenciamento de Riscos

- Elaborar e documentar as políticas e estratégias para o gerenciamento do risco operacional;

- Implementar estrutura, disseminar o conhecimento e subsidiar as demais áreas para aderência e comprometimento das regulamentações que visam o gerenciamento de risco operacional;
- Auxiliar na definição de apetite de risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;
- Aplicar metodologia para identificar, avaliar, monitorar, mensurar, controlar e mitigar continuamente as causas, dos eventos de risco operacional, junto aos gestores;
- Monitorar o gerenciamento dos riscos da 1° linha de defesa;
- Elaborar relatório de Risco Operacional com periodicidade mínima anual e submeter ao Comitê de Risco;
- Documentar, armazenar, classificar e agregar as informações referentes às perdas associadas ao risco operacional;
- Identificar previamente os riscos inerentes a novos produtos e serviços, bem como em produtos e serviços existentes, mudanças significativas em processos, sistemas, operações, modelo de negócio e reorganizações societárias significativas;
- Disseminar à instituição, em seus diversos níveis, o apetite a risco documentado na RAS, bem como o procedimento para reporte de ocorrência relacionadas a não observância dos níveis de apetite por riscos.

7.7. Da Área de Controles Internos

- Modelar novos processos operacionais ou atuar na reengenharia de processos e atividades existentes;
- Avaliar a eficiência dos controles internos com base em riscos;
- Apoiar na estruturação e gestão dos riscos corporativos;
- Fortalecer no processo de prevenção de fraude corporativa;
- Apoiar a manutenção de processos operacionais alinhados com a estratégia e apetite a risco da instituição.

7.8. Da Área de Compliance

- Monitorar riscos específicos, como, por exemplo, a não conformidade com leis e regulamentos aplicáveis a instituição;
- Reportar eventuais inconsistências diretamente a Diretoria Executiva;
- Orientar sobre processos de gerenciamento de riscos e conformidade;
- Identificar mudanças no cenário regulatório e de riscos, e alertar a 1ª Linha de Defesa de tais inovações;
- Realizar testes e avaliação de aderência das atividades institucionais às normas legais, infralegais, às recomendações emitidas por órgãos de supervisão e autorreguladores,

assim como às políticas internas, conforme plano anual de testes de conformidade aprovado pela Diretoria Executiva;

- Auxiliar na definição de apetite de risco e na tomada de decisão nos negócios do dia a dia, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;
- Identificar e reportar ao COAF os atos, omissões e operações que possam auxiliar ou cooperar de alguma forma para a identificação dos delitos de fraude, lavagem de dinheiro e/ou financiamento ao terrorismo;
- Elaborar treinamentos e ações de disseminação de cultura de conformidade e controle de riscos.

7.9. Da Área de Segurança da Informação

- Identificar, classificar, documentar processos críticos de negócio, bem como avaliar potenciais impactos decorrentes de interrupção dos mesmos;
- Estabelecer estratégias para assegurar a continuidade das atividades da instituição;
- Elaborar planos de continuidades de negócios que estabeleçam procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como as ações de comunicação necessárias;
- Realizar testes e revisões dos planos de continuidade de negócios com periodicidade adequada;
- Assegurar a integridade, segurança e disponibilidade de dados e dos sistemas de informação utilizados, sendo adequados às necessidades e às mudanças do modelo de negócio, incluindo mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade de ataques digitais;
- Implementar estrutura de governança de TI consistente com os níveis de apetite por riscos estabelecidos na RAS.

7.10. Da Área de Antifraude

- Prevenir, identificar e responder a fraudes bancárias;
- Proteger os ativos do Grupo e dos seus clientes;
- Informar à Unidade de Gerenciamento de Riscos os eventos de risco operacional.

7.11. Dos Gestores e Colaboradores

- Identificar os riscos operacionais oriundos do exercício de suas atividades, considerando também os serviços terceirizados utilizados;
- Estabelecer e gerenciar os controles de risco inerentes as suas atividades do dia a dia.
- Avaliar regularmente o serviço pactuado com prestadores de serviços terceirizados;
- Informar à Unidade de Gerenciamento de Riscos os eventos de risco operacional.

7.12. Do Jurídico

- Identificar e mitigar o risco legal na elaboração dos contratos firmados pela instituição;
- Incluir nos contratos firmados pela instituição cláusulas que estabeleçam claramente os papéis e as responsabilidades dos prestadores de serviços terceirizados;
- Garantir a inclusão das cláusulas necessárias nos contratos de TI conforme Resolução N° 4.893.

8. DIRETRIZES DE GERENCIAMENTO DE RISCO OPERACIONAL

A metodologia utilizada está em linha com o *framework* definido nos documentos: (i) "*Principles for the Sound Management of Operational Risk"* emitido em junho de 2011 pelo *Basel Committee on Banking Supervision* e (ii) "*Integrated Framework: Application Techniques"* publicado em setembro de 2011 pelo COSO - *Committee of Sponsoring Organizations of the Treadway Commission*. Neste modelo, a gestão de riscos operacionais considera os seguintes elementos:

- Ambiente Interno
- Fixação de Objetivos
- Identificação de Eventos
- Avaliação de Riscos
- Atividade de Controle
- Resposta a Risco
- Informações e Comunicações
- Monitoramento

Desta forma, o Conglomerado Genial institui um ambiente interno propício para a prática de controles internos e gestão de riscos onde os objetivos estratégicos são fixados, os eventos de risco identificados e avaliados e uma resposta para a ocorrência dos riscos mapeados é estabelecida. A Genial possui atividades de controle, um fluxo de informações e comunicações e, por fim, um monitoramento contínuo dos riscos relevantes.

9. METODOLOGIA

9.1. Identificação

O primeiro componente da gestão de riscos operacionais diz respeito ao conhecimento dos riscos aos quais as empresas do grupo estão expostas e tudo tem início no processo de mapeamento das deficiências. As ferramentas adotadas pelas áreas de Controles Internos são: (i) Identificação dos eventos de perdas - Base de Perdas e (ii) Control Risk Self Assessment - CRSA.

A área de Risco possui uma base de dados para documentar e armazenar as informações referentes às perdas associadas ao risco operacional, incluindo provisões, perdas associadas a risco de mercado e/ou risco de crédito, e despesas relacionadas a cada evento, e outros dados, caso aplicável, com objetivo de gerenciar o risco operacional e construir uma base histórica. Os registros são efetuados considerando os seguintes requisitos mínimos:

- Registro de eventos de perda (Individual) acima de R$ 1.000,00;
- Registro de eventos da mesma origem ou natureza que, de forma agregada ocorridos no mesmo dia, seja superior a R$ 1.000,00;
- Justificativa dos eventos de perda acima de R$10.000.

O Control Risk Self Assessment – CRSA consiste em reunir os gestores ou responsáveis para entrevistas e discussões sobre assuntos ou processos específicos de suas áreas de atuação, com a finalidade de produzir uma autoavaliação dos processos, riscos e controles existentes e desenvolver planos de ação para mitigá-los, quando aplicável. O resultado desta análise é a base para a elaboração da matriz de riscos.

9.2. Avaliação e Mensuração

Este processo consite na quantificação ou dimensionamento da exposição ao risco operacional com o objetivo de avaliar o impacto nos negócios da empresa. Envolve a estimativa da probabilidade de ocorrência e impacto de forma a determinar o nível de risco. Nas tabelas abaixo são apresentadas as definições de probabilidade e impacto, respectivamente, adotadas pela Instituição:

PROBABILIDADE	**REMOTA**	**POSSÍVEL**	**PROVÁVEL**
FREQUÊNCIA	Há possibilidade de ocorrer de forma infrequente e incomum	Há possibilidade de ocorrer em algumas circunstâncias.	Possivelmente ocorra com frequência.

IMPACTO	**BAIXO**	**MÉDIO**	**ALTO**
FINANCEIRO (valores em Reais R$)	Perdas financeiras: **de: 0,01 até 1.000.000,00**	Perdas financeiras: **de: 1.000.000,01 até 10.000.000,00**	Perdas financeiras: **acima de 10.000.000,00**

IMAGEM	Menções negativas de baixa relevância: **Veículos de comunicações locais**	Menções negativas de média relevância: **Veículos de comunicações regionais e estaduais**	Menções negativas relevantes: **Veículos de comunicações nacionais e redes sociais**
CLIENTE	Indisponibilidades afetando até: **De 01% até 10% dos clientes**	Indisponibilidades afetando até: **de 11% até 25% dos clientes**	Indisponibilidade afetando: **Acima de 25% dos clientes**
LEGAL / COMPLIANCE	**Aplicação de Sanções de baixa relevância**, sem efeito midiático nem de imagem.	**Aplicação de sanções de média relevância,** podendo haver menção midiática pontual, com pequeno a médio potencial de dano a imagem.	**Aplicação de sanções relevantes,** com menção midiática relevante e dano à reputação causando empecilhos à concretização de negócios.

A tabela abaixo demonstra a **Exposição** ou **Grau de Risco** da relação probabilidade *versus* impacto:

IMPACTO

PROBABILIDADE	#	**BAIXO**	**MÉDIO**	**ALTO**
	REMOTA	RB	RB	RM
	POSSÍVEL	RB	RM	RA
	PROVÁVEL	RM	RA	RA

Onde:

- RB (Risco Baixo)
- RM (Risco Moderado)
- RA (Risco Alto)

A Instituição define quatro respostas aos riscos mapeados:

EVITAR	MITIGAR	TRANSFERIR	ACEITAR
•Descontinuação das atividades que geram determinado risco.	•São adotados medidas e controles para reduzir a probabilidade ou o impacto dos riscos não tolerados e não controlados. Se necessários são alterados processos, sistemas e/ou pessoas.	•Redução da probabilidade ou do impacto dos riscos pela transferência ou pelo compartilhamento do risco. Como aquisição de seguros e/ou terceirização de uma atividade.	•Nenhuma medida é adotada para afetar a probabilidade ou o grau de impacto dos riscos. A Instituição aceita certo nível de risco devido ao custo para a mitigação ou irrelevância do risco.

9.3. Controle

Consiste na realização de testes na Matriz de Riscos e Controles com o objetivo de avaliar a aderência dos controles aos riscos envolvidos.

9.4. Monitoramento e Reporte

Monitoramento é a ação que tem por objetivo identificar as deficiências do processo de gestão do risco operacional de forma que as fragilidades detectadas sejam levadas ao conhecimento da Alta Administração.

A área de Risco e Controles Internos elaboram os relatórios periódicos formalizando as deficiências de controles e exposições de risco, base de perdas, adesão do risco incorrido aos termos da RAS e resultados dos testes e das revisões do “Plano de Continuidade de Negócios”.

10. REVISÃO E APROVAÇÃO

Esta política deve ser revisada pelo Comitê de Risco e aprovada pela Diretoria Executiva no mínimo anualmente.

Classificação: Pública

RIO DE JANEIRO
PHONE:
55 21 3923-3000
3500-3000

SÃO PAULO
PHONE:
55 11 3206-8000
2920-8000

MIAMI AFFILIATE
PHONE:
1 212 388-5600

NEW YORK
PHONE:
1 212 388-5600