STRIVO GESTÃO DE RECURSOS S.A.

# PLANO DE CONTINUIDADE DO NEGÓCIO

Versão 2.0
Vigência Maio/2025

| Atividade | Área |
|---|---|
| Elaboração | Direção de Compliance |
| Revisão | Comitê de Compliance |
| Aprovação | Comitê de Compliance |

Classificação das Informações:
Uso Interno/**Uso Público**

## 1. Introdução

Este Plano de Continuidade do Negócio ("PCN") se aplica à administradora de carteira de títulos e valores mobiliários, na modalidade gestora de recursos, nos termos da regulatórios editados pela Comissão de Valores Mobiliários ("CVM"), Strivo Gestora de Recursos S.A., doravante denominada "Strivo" ou "Gestora".

Pelo presente documento, a Strivo define seu PCN que estabelece estratégias e procedimentos a serem observados na eventualidade de incidentes ou emergências que envolvam a Gestora e/ou seus sócios, diretores, empregados, funcionários, trainees, estagiários, prestadores de serviços que venham, de maneira direta ou indireta, trabalhar para a Strivo e todos que, de alguma forma, auxiliam o desenvolvimento das atividades da Gestora ("Membros").

Em decorrência disto, é entendimento corrente que o bem mais precioso da Strivo é o patrimônio dos clientes sob gestão e as informações estratégicas decorrentes, com inequívoca prioridade sobre os ativos organizacionais. Portanto, assegurar aos clientes que os seus patrimônios não serão afetados por eventos cujo grau de previsibilidade seja nulo, mas de altíssimo impacto nas operações organizacionais mais críticas, é a essência e objetivo principal do trabalho em curso.

O uso pretendido do PCN é minimizar o impacto de um acontecimento inesperado que poderia apresentar inacessibilidade às instalações da Gestora.

Por fim, recomenda-se a leitura deste PCN em conjunto com a Política de Segurança da Informação, Política de Segregação de Segregação de Atividades, e Política de Segurança Cibernética, sobretudo em decorrência das regras estabelecidas pela Strivo.

## 2. Objetivos

A PCN da Strivo tem por objetivo estabelecer as medidas a serem tomadas para identificar e prevenir as possíveis contingências que poderão trazer um impacto negativo considerável sobre a condução das atividades da Gestora. Dentre estas contingências se incluem, por exemplo, crises econômicas, falhas operacionais ou desastres naturais.

Como estratégia para atingir nosso objetivo principal, definimos como objetivos específicos:

a) Realizar backup externo e diário de todo o banco de dados, envolvendo todas as operações diárias, incluindo os arquivos de programas;

b) Assegurar a integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações;

c) Manter os sistemas operacionais disponíveis; e

d) Manter rede eletrônica em funcionamento e em boas condições operacionais.

Para redução e controle de eventuais perdas com contingências, todos os membros da Strivo deverão conhecer os procedimentos de backup e salvaguarda de informações (confidenciais ou não), planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho.

**3. Princípios Norteadores**

A Strivo, pautada pelos deveres de diligência e cuidado e pela respeitabilidade que norteiam a condução dos seus negócios, em casos de ocorrência de quaisquer eventos ou sinistros que possam inviabilizar, paralisar ou comprometer temporariamente o exercício de suas atividades seguirá os procedimentos aqui definidos ou, nos casos não previstos neste plano, os procedimentos estabelecidos pela sua diretoria.

A Strivo, por meio do presente PCN, buscará sempre identificar e prevenir os riscos relacionados ao seu negócio sejam eles físicos, patrimoniais ou financeiros.

**4. Diretrizes de Prevenção e Contingências**

Para a eficaz implementação desta Política, a Strivo buscará conhecer e reparar os principais pontos de vulnerabilidade de suas instalações e equipamentos. Para tal finalidade tomará medidas que a permitam:

a. Conhecer e minimizar os danos no período pós-contingência;

b. Minimizar as perdas para si, seus clientes e Colaboradores advindos da interrupção de suas atividades; e

c. Normalizar o mais rápido possível as atividades da Gestora.

Em linhas gerais, os passos para execução deste plano são os seguintes:

a. Identificação das interdependências entre as instalações, equipamentos e processos de negócios da Strivo com outras empresas e/ou com fornecedores e contratados;

b. Listagem das diferentes atividades da Strivo e identificação daquelas com alto interesse estratégico e/ou aquelas com elevado potencial de risco financeiro, físico ou operacional;

c. Listagem das instalações, equipamentos, fornecedores, contratados que podem representar dificuldades ou restrição à aplicação deste plano; e

d. Verificação da adequação dos meios preventivos e de proteção às características da operação e de negócio da Strivo.

**5. Análise de Riscos**

Definimos como foco o desenvolvimento de um plano de ação que assegure a continuidade das atividades operacionais na Strivo, mesmo nos eventos de maior ruptura operacional, independentemente do se seu nível de risco de ocorrência.

Outra consideração que fundamenta a opção da Strivo por analisar risco sobre os recursos abaixo, prende-se ao objetivo exclusivo de manter ou restabelecer rapidamente a gestão e controle do patrimônio dos clientes.

Considera-se, conceitualmente, risco como sendo: "a probabilidade de ocorrência de um evento indesejado e ou imprevisível causando graves rupturas operacionais e consequente prejuízo patrimonial". Assim: **RISCO = PROVABILIDADE DO EVENTO x CONSEQUENCIA**

Neste contexto, nossa análise de risco se concentra em avaliar eventos que provoquem danos aos recursos abaixo:

a) Segurança, integridade, qualidade e acessibilidade aos dados e informações;

b) Corpo técnico;

c) Tecnologia das informações; e

d) Instalações.

A avaliação dos riscos aos quais a Strivo, na execução das suas atividades cotidianas, se expõe, podem ser analisadas sob três aspectos:

I) A PROBABILIDADE de que o evento produza rupturas graves;

II) A GRAVIDADE das possíveis consequências prejudiciais; e

III) O ÍNDICE de exposição aos riscos.

A probabilidade de consequências prejudiciais aumenta com a maior exposição. Por isso, a exposição deve ser considerada como outra dimensão de probabilidade.

A avaliação de riscos considera a probabilidade e a gravidade da consequência prejudicial, determinando o potencial de perdas, conforme abaixo:

| Probabilidade do Evento | | |
|---|---|---|
| **Definição Qualitativa** | **Significado** | **Pontuação** |
| **Frequente** | **Ocorrência Provável (Evento Frequente)** | **5** |
| **Ocasional** | **Provável Que Ocorra (Eventos Ocasionais)** | **4** |
| **Remoto** | **Improvável, Porém Possível de Ocorrer (Ocorre Raramente)** | **3** |
| **Improvável** | **Muito Improvável Que Ocorra (Sem Registro de Eventos Anteriores)** | **2** |
| **Extremamente Improvável** | **Quase Inconcebível que o Evento Ocorra** | **2** |

Avaliada a probabilidade de ocorrência do evento, passamos a avaliar a severidade das consequências do evento que regem o grau de urgência da medida de segurança operacional requerida, conforme abaixo:

| Probabilidade do Evento | | |
|---|---|---|
| **Definição** | **Significado** | **Classificação** |
| **Gravíssimo** | **Destruição de equipamentos e instalações, Mortes múltiplas.** | **A** |
| **Grave** | **Destruição de equipamentos. Instalações inacessíveis.** | **B** |
| **Médio** | **Equipamentos parcialmente comprometidos. Acessos limitados.** | **C** |
| **Baixo** | **Instalações e equipamentos operacionais. Uso alternativo de redes.** | **D** |
| **Insignificante** | **Consequências leves.** | **E** |

[*ESPAÇO INTENCIONALMENTE DEIXADO EM BRANCO*]

A partir da análise de probabilidade e severidade dos eventos podemos construir uma matriz de avaliação de riscos, como a que se apresenta abaixo, que é a ferramenta utilizada para ordenar em grau de prioridade os riscos que requerem mais atenção:

| Severidade do Risco | | | | | |
|---|---|---|---|---|---|
| Probabilidade do Risco | Gravíssimo A | Grave B | Médio C | Baixo D | Insignificante E |
| Frequente 5 | 5A | 5B | 5C | 5D | 5E |
| Ocasional 4 | 4A | 4B | 4C | 4D | 4E |
| Remoto 3 | 3A | 3B | 3C | 3D | 3E |
| Improvável 2 | 2A | 2B | 2C | 2D | 2E |
| Extremamente Improvável 1 | 1A | 1B | 1C | 1D | 1E |

Com base nas avaliações de riscos podemos ordená-los por prioridade orientada pelos critérios de aceitabilidade dos riscos que seguem: (i) Aceitável: quando não é necessário adotar medidas mitigatórias, a menos que se possa reduzir mais o risco com pouco custo ou esforço; (ii) Tolerável: a organização está preparada para suportar o risco. Medidas mitigatórias são recomendadas; (iii) Intolerável: condições que impliquem em cessar as operações até que o risco se reduza ao nível tolerável.

| Gestão de Risco | Índice de Avaliação de Risco | Critério de Aceitabilidade |
|---|---|---|
| Intolerável | 5A; 5B; 5C; 4A; 4B; 3A | Inaceitável sob as circunstâncias existentes |
| Tolerável | 5D; 5E; 4C; 4D; 4E; 3B; 3C; 3D; 2A; 2B; 2C | Aceitável com mitigação de risco. Pode requerer uma decisão direta. |
| Aceitável | 3E; 2D; 2E; 1A; 1B; 1C; 1D; 1E | Aceitável. |

Não existe 100% (cem por cento) de segurança operacional, ou segurança absoluta. São necessárias ações continuadas com objetivo de manutenção dos riscos nos seus mais baixos níveis. Ao considerar um determinado risco intolerável ou tolerável, faz-se necessário a adoção de medidas mitigadoras. Quanto mais elevado o risco, maior a urgência. A redução de risco se dá pela redução da gravidade das consequências, da probabilidade ou da exposição.

A Strivo tem de forma consolidada algumas ações mitigatórias de risco, que buscam assegurar sua operacionalidade, permitindo que os riscos a que se expõe, conforme cenários abaixo, sejam classificados como “toleráveis”:

a) “Backup” externo, diário e automático, com redundância em equipamentos localizados fora do continente onde a gestora opera;

b) “Backup” extensivo a todos os aplicativos e arquivos de programas em uso na organização (incluindo registro dos e-mails);

c) “Data Center” contratado, permitindo comunicação e acesso remoto para dados, aplicativos e arquivos de programa;

d) Toda a documentação que represente obrigações e haveres da Strivo é digitalizada, respeitadas as regras de segregação, detalhadas na Política de Segurança da Informação, e Política de Segurança Cibernética;

e) Todos os documentos, arquivos e pastas criadas, usadas e/ou atualizadas no dia a dia são automaticamente salvas no servidor para posterior “backup”;

f) A área de compliance mantém registro atualizado de todas as senhas de acesso aos softwares de gestão usados pela Strivo;

g) Contrato terceirizado de manutenção de TI com presença rotineira na Strivo e atendimento especial em casos de necessidade; e

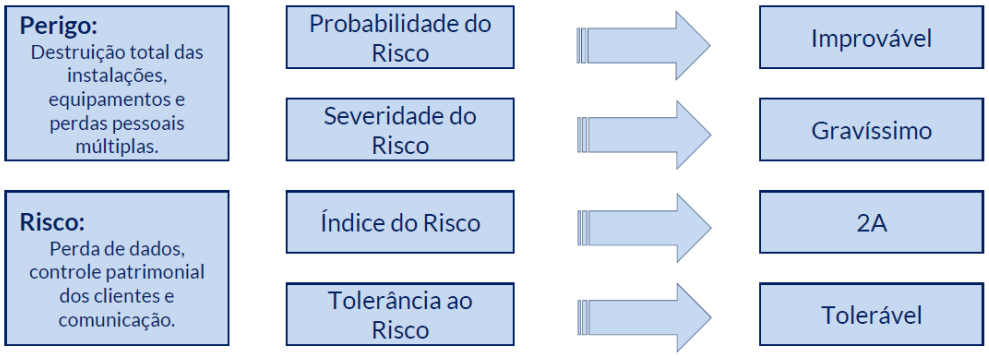
h) Redundância no serviço de internet (duas operadoras contratadas simultaneamente), evitando o risco de o sistema ficar fora do ar.

**6. Identificação de Eventos vs. Riscos**

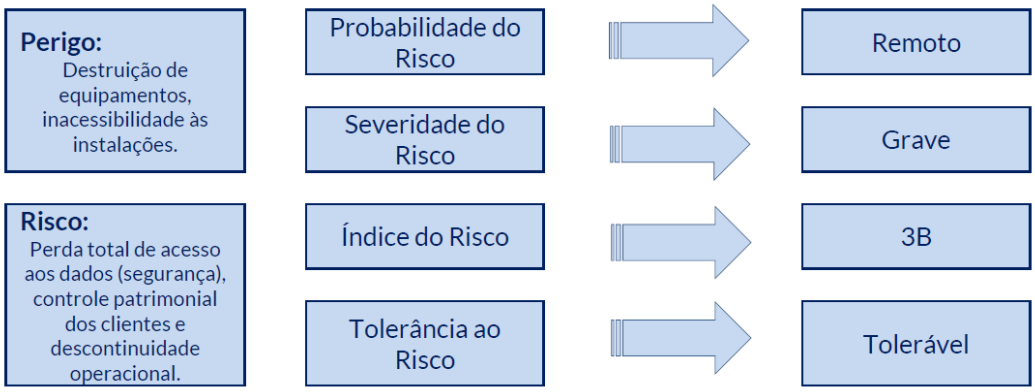
Ao avaliarmos os eventos possíveis, focamos em efeitos que possam comprometer dados e informações sobre o patrimônio dos clientes, pessoas, informática e comunicação e instalações físicas.

Estes são os mais importantes, e imprescindíveis, fatores de continuidade dos negócios na Strivo.

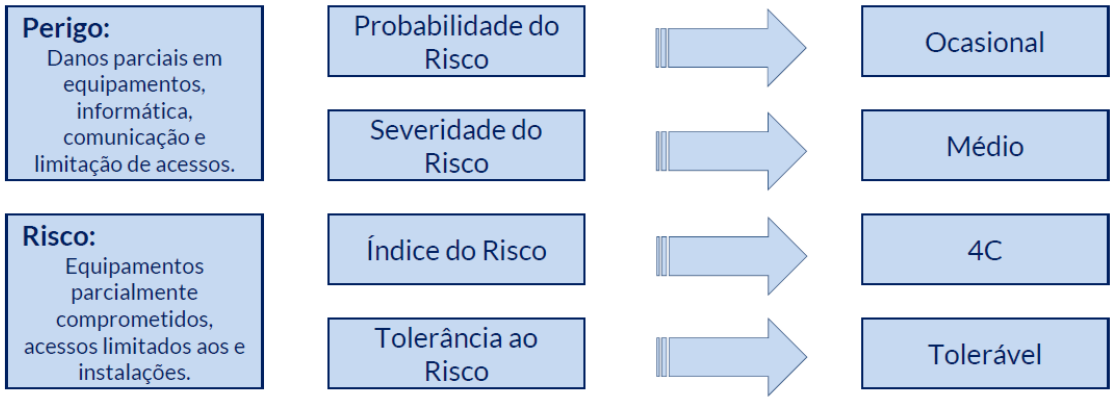
a) Cenário Hipotético 1: Ocorrência de eventos naturais e ou acidente de grandes proporções com sérios danos nas instalações físicas, equipamentos de informática, sistema de comunicação e perdas pessoais múltiplas.



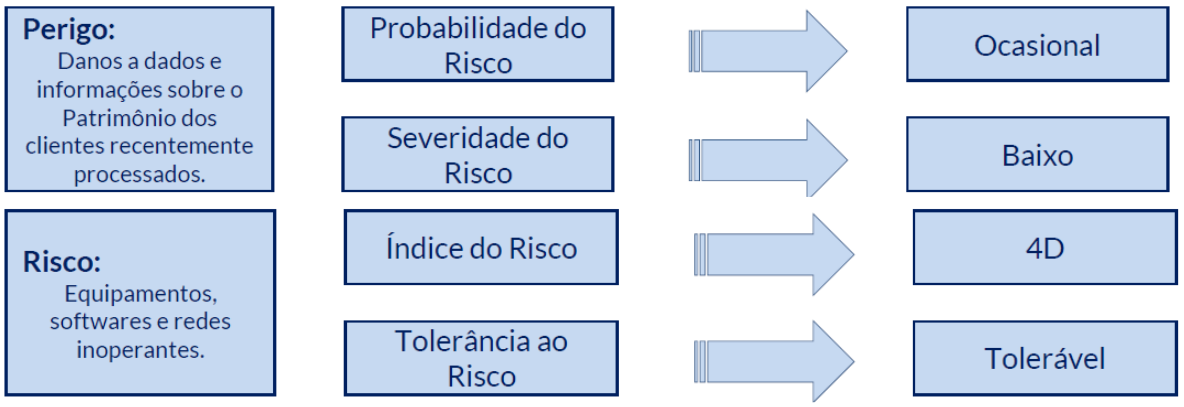

b) Cenário Hipotético 2: Acidente no entorno das instalações e ou distúrbios sociais de grandes proporções ocasionando destruição de equipamentos e ou tornando as instalações inacessíveis.




c) Cenário Hipotético 3: Evento acidental provocando danos parciais nos equipamentos, com comprometimento parcial dos sistemas de informática e de comunicação, provocando limitações e restrições de acesso às instalações físicas.




d) Cenário Hipotético 4: Em caso de acidente originado por causas naturais ou humanas em que haja interrupção no fornecimento de energia por tempo muito superior ao de suporte dos "*no breaks*", causando ruptura no funcionamento dos equipamentos e redes de comunicação.




**7. Plano Preventivo**

Os elementos estratégicos da Strivo a serem protegidos a proteger são, principalmente, o constante desenvolvimento técnico de seus colaboradores, a confiabilidade de seus sistemas de informação e a manutenção da segurança e confiabilidade das instalações da Gestora.

**8. Plano de Administração de Crises**

Neste tópico mapeamos os procedimentos planejados e que serão adotados enquanto perdurar a situação de crise, até a total normalidade operacional da organização. Definimos também um passo a passo de todas as ações desde uma "Declaração de Situação de Emergência" à execução das ações que vise retomada imediata das operações em todas as áreas da Strivo.

A Strivo conduz suas operações num espaço total de 108 m² (cento e oito metros quadrados), observadas as regras de segregação consolidadas na Política de Segurança da Informação, Política de Segurança Cibernética e Política de Segregação de Atividades. Analisados os riscos a que se expõe e são toleráveis com mitigação, o plano terá a simplicidade e funcionalidade adequada.

a) O que é essencial para a manutenção das operações?

Pela peculiaridade operacional prestar serviço de administração de carteiras de valores mobiliários, exclusivamente na categoria "gestor de recursos", onde a guarda de valores, títulos, registros e precificação de ativos são operações externas, realizadas por Bancos Custodiantes, define-se como essencial às operações da Strivo o que segue:

i) Pessoas em geral, com atenção especial aos gestores, *back office* e *risk control*;

ii) Segurança, integridade e acessibilidade dos dados e informações referentes ao patrimônio dos clientes;

iii) Redes de comunicação de dados e voz;

iv) *Softwares* de gestão e controles;

e) *Hardwares* compatíveis com as exigências operacionais dos softwares e redes;

f) Recuperação dos dados e informações geradas nas últimas 24 horas anteriores ao evento de ruptura operacional.

b) Central de Crise

Em caso de evento com rupturas operacionais será instalada uma central de crise em local determinado pela Diretoria de *Compliance* e Risco, de fácil acesso a todos os Membros da organização.

c) Pessoas e Ações

A implementação dos planos de contingência deverá ser realizada em até quatro horas e será de responsabilidade do Diretor de Compliance e Riscos, observadas as atribuições adiante:

i) Diretor de Compliance e Riscos

- Declaração de crise operacional e coordenação do PAC;

- Verificar e validar a segurança, integridade e acessibilidade dos dados capturados e arquivados pelo sistema de "backup" diário.

ii) Equipe de *Back Office*:

-Ativar serviços de TI contratados previamente;

- Ativar técnicos responsáveis por manutenção e funcionalidade dos hardwares e softwares;
- Garantir pleno funcionamento da Política de Segurança de TI, inclusive com fornecimento emergencial de equipamentos completos: desktops e notebooks com o objetivo de, ainda que por aquisição em regime de urgência, fornecer no mínimo 01 (um) *moden* banda larga que restabeleça, mesmo que precariamente, as comunicações via rede.

- Atualizar e ou recuperar dados e informações não capturados no último "backup" disponível no "Data Center";
- Dar continuidade às operações.

d) Testes de Contingência

Os testes de contingências possibilitam que a Strivo esteja preparada, proporcionando condições adequadas para continuar suas operações. Sendo assim, anualmente, será solicitado pela Diretoria de Compliance e Risco um teste de contingência para verificar:

i) Acesso aos sistemas;
ii) Acesso ao e-mail corporativo;
iii) Acesso aos dados armazenados; e
iv) Qualquer outra atividade necessária para continuidade do negócio.

**9. Plano de Recuperação do Negócio**

A Strivo mantém mapeado seus principais processos de negócios, de forma que em caso de ocorrência de contingências seja possível retomar as operações com os menores custos de transação, perdas de tempo e de recursos físicos e materiais possíveis.

Para a retomada célere e eficaz das operações após uma contingência, a Strivo manterá procedimentos que a permitem:

a) Utilizar alternativas de dentro ou fora da Zenith para substituição ou reparação de equipamentos danificados, tais como uma lista de fornecedores capazes de auxiliar neste tipo de situação;

b) Manter o gerenciamento do pessoal e os procedimentos das operações administrativas mesmo durante os efeitos da contingência;

c) Retornar definitivamente a utilização das instalações de sua sede após a ocorrência da contingência; bem como

d) Avaliar as perdas da interrupção dos negócios.

**10. Tratamento de Contingências**

Para o tratamento das contingências diretamente relacionadas com a operação dos negócios da Strivo, deverão ser mantidos sempre atualizados procedimentos que permitam à Gestora:

a) Aumentar rapidamente seu contingente de pessoal técnico qualificado e/ou fornecedores caso a demanda por seus serviços aumente rapidamente sem que isso implique na queda da qualidade da prestação dos serviços;

b) Identificar novos potenciais mercados de atuação e/ou produtos caso haja queda, ou longos períodos de recessão, na demanda de seus clientes atuais;

c) Manter-se sempre competitiva e inovadora, de forma a evitar a perda de sua participação no mercado, com a exploração de seus pontos fortes e com a constante diminuição de seus pontos fracos;

d) Valer-se de suas vantagens competitivas no mercado;

e) Ampliar constantemente sua base de clientes, de forma que seja mantido o grau de pulverização na carteira de clientes adequado ao porte da Strivo e a manutenção da confiabilidade e qualidade dos serviços prestados;

f) Manter um fluxo de caixa que seja hábil para fazer frente às despesas imprevisíveis. O edifício da sede onde se encontra a Strivo tem gerador para as áreas internas e comuns ao condomínio;

g) A gestora também conta com a contingência das Administradoras Fiduciárias com quem possui relação comercial/operacional para o registro de dados e operações realizadas pela Gestora, proporcionando continuidade da operação caso alguma catástrofe ocorra na Strivo;

h) Na hipótese de impedimento do Diretor de Gestão de continuar a exercer às suas atividades a Strivo possui no seu quadro de Colaboradores, outros gestores credenciados na CVM capazes de substituir de imediato esse diretor; e

i) Em caso de impedimento de um de seus Administradores Fiduciários, a Strivo mantém relacionamentos com outras instituições financeiras que poderão vir a substituir a atual, sendo que nada data de confecção desta Política, a Strivo estava habilitada em cinco prestadores de serviços fiduciários para o fim mencionado neste item.

**11. Plano de Recuperação de Desastres**

A Strivo possui estratégia para os diversos tipos de adversidades que possam surgir na sua infraestrutura tecnológica, conforme detalhado na Política de Segurança Cibernética e Política de Segurança da Informação.

**12. Disseminação do Plano**

Para redução e controle de eventuais perdas com contingências, todos os Colaboradores da Strivo deverão conhecer os procedimentos de *backup* e salvaguarda de informações (confidenciais ou não, planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho os quais serão elaborados e divulgados pela Diretoria de Compliance e Risco.

**13. Vigência & Revisões**

Esta Política entra em vigor em **01/05/2025**, revoga todas as versões anteriores, devendo ser revisada anualmente ou, havendo necessidade anterior, o que for menor, para que o documento permaneça atualizado e aderente à legislação e regulação aplicável.

A aérea de compliance informará oportunamente aos Membros sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da Gestora na rede mundial de computadores.

**14. Disposições Finais**

A Diretora da Strivo responsável pela prevenção de perdas e implementação dos Planos descritos neste documento é a **Sra. Natália Bertol**, Diretora de Compliance e Risco da Gestora.