POLÍTICA DE *COMPLIANCE* E CONTROLES INTERNOS;

POLÍTICA DE CERTIFICAÇÃO E

POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E CYBERSEGURANÇA

MAXIPLAN LTDA.

Versão: 02
Data: 13/05/2020

1. Política de *Compliance* e Controles Internos

1.1 Objetivo

Formalizar os procedimentos para gerenciamento dos riscos de *compliance* e controles internos na MAXIPLAN LTDA. ("GESTORA").

1.2 A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a GESTORA (doravante, "Colaboradores").

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de *Compliance*.

1.3 Estrutura e Responsabilidades

Cabe à GESTORA garantir, por meio de regras, procedimentos e controles internos adequados, o permanente atendimento à legislação, regulação, autorregulação e políticas internas vigentes.

Todos devem adotar e cumprir as diretrizes e controles aplicáveis à GESTORA contidas nesta Política, zelando para que todas as normas éticas, legais, regulatórias e autorregulatórias sejam cumpridas por todos aqueles com quem são mantidas relações de cunho profissional, comunicando imediatamente qualquer violação ou indício de violação ao Diretor de *Compliance*.

a) Cabe à alta administração da GESTORA:

- A responsabilidade pelos controles internos e o gerenciamento dos riscos de *compliance*;
- Indicar um diretor estatutário responsável por *compliance* e controles internos[1], devendo tal profissional ter acesso a todas as informações e pessoas na GESTORA quando do exercício de suas atribuições;
- Aprovar, estabelecer e divulgar esta Política; e
- Garantir a efetividade do gerenciamento do risco de *compliance*.

b) O Diretor de *Compliance* deve:

- Auxiliar a alta administração a assegurar a efetividade do Sistema de Controles Internos e *Compliance* da GESTORA, atuando no gerenciamento efetivo de tais atividades no seu dia-a-dia;
- Gerenciar o Comitê de *Compliance* e o Conselho de Ética, garantindo seu adequado funcionamento e o registro em ata das decisões tomadas;
- Designar os secretários das reuniões do Comitê de *Compliance* e do Conselho de Ética;
- Monitorar e exercer os controles e procedimentos necessários ao cumprimento das normas.

[1] Com capacidade técnica e função independente das relacionadas à administração de carteiras de valores mobiliários, ou em qualquer atividade que limite a sua independência, na instituição ou fora dela.

É responsabilidade de todos os Colaboradores o cumprimento das normas legais, regulatórias e autorregulatórias aplicáveis às suas atividades, bem como de todas as normas internas da GESTORA.

Qualquer suspeita, indício e/ou evidência de desconformidade por eles verificada deve ser imediatamente comunicada ao Diretor de *Compliance*.

O Diretor de *Compliance* se reporta apenas à alta administração da GESTORA, com autonomia e independência para indagar a respeito de práticas e procedimentos adotados nas suas operações/atividades, devendo adotar medidas que coíbam ou mitiguem as eventuais inadequações, incorreções e/ou inaplicabilidades.

Os controles e monitoramentos determinados nesta Política são prerrogativa exclusiva dos integrantes da Área de *Compliance* da GESTORA, sendo exercidos de forma autônoma e independente, com ampla liberdade de discussão e análise dos temas sob sua responsabilidade: o Diretor de *Compliance* tem poder de veto – mas não *de voto* – nos Comitês de negócios da GESTORA.

A Área de *Compliance* é formada pelo diretor estatutário o qual se dedica ao exercício das atividades de cumprimento de regras, políticas, procedimentos e controles internos, incluindo o cumprimento das normas relativas ao combate e prevenção à lavagem de dinheiro, ao financiamento do terrorismo e à corrupção (organograma anexo).

1.4 Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, se necessário em virtude de mudanças legais/ regulatórias/ autorregulatórias.

1.5 Escopo e Atribuições do *Compliance*

A atuação do Diretor de *Compliance* tem por escopo:

a) Temas Normativos:

- Controlar a aderência a novas leis, regulação e normas de autorregulação aplicáveis à GESTORA e às suas atividades, e apresentar o resultado de suas verificações no Comitê de *Compliance*;
- Controlar e monitorar as licenças legais e certificações necessárias, e a sua obtenção/ renovação manutenção junto às autoridades reguladoras/ autorreguladoras competentes;

- Auxiliar a alta administração da GESTORA no relacionamento com órgãos reguladores, e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;
- Realizar testes internos, revisões e relatórios obrigatórios nas frequências definidas nas políticas e manuais internos, bem como na legislação, regulação e autorregulação em vigor.

b) Boas Práticas

- Disseminar e promover as informações necessárias para o cumprimento das políticas internas e das normas legais, regulatórias e de autorregulação aplicáveis;
- Exercer seu controle, garantindo que as políticas e manuais pertinentes estejam atualizados e mantidos em diretório acessível a todos que delas devam ter conhecimento;
- Disponibilizar aos novos Colaboradores as políticas internas aplicáveis, e coletar os termos de ciência e aderência por eles assinados;
- Estabelecer controles para que todos os Colaboradores da GESTORA que desempenhem funções ligadas à gestão de fundos de investimento ou de carteiras administradas atuem com independência[2];
- Garantir que os controles internos sejam compatíveis com os riscos da GESTORA em suas atividades[3];
- Analisar informações, indícios ou identificar, administrar e, se necessário, levar temas para análise e deliberação no Comitê de *Compliance* e/ou no Conselho de Ética;
- Orientar previamente e/ou acompanhar o responsável pela comunicação à imprensa em contatos telefônicos, entrevistas, publicação de artigos ou qualquer outra forma de manifestação de opinião através de veículo público (inclusive na internet).

c) Governança

- Aprovar novas políticas internas no Comitê de *Compliance*, ou a sua revisão, por força de mudanças na legislação, regulação ou autorregulação aplicáveis, ou ainda, de decisões internas da GESTORA;
- Aprovar a oferta de novos produtos e prestação de novos serviços pela GESTORA, a partir de inputs técnicos do Comitê de Investimento;
- Atuar para que haja efetividade na segregação física de atividades conflitantes;
- Apresentar o resultado de seus controles e verificações no Comitê de *Compliance*;
- Monitorar e buscar a efetiva aplicação dos documentos de *compliance* e controles internos abaixo listados;
- Servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética e Conduta Profissional da GESTORA e às demais políticas da GESTORA;
- Convocar, gerenciar, organizar e secretariar o Comitê de *Compliance*, registrando suas decisões em atas;
- Implementação de Regras e Guarda de Evidências – monitoramento da implementação de procedimentos, de cumprimento das normas e políticas internas, bem como de mecanismos de guarda de evidências;
- Salvaguarda de Informações – devem ser mantidos, pelo prazo mínimo de 5

[2] E atentem ao seu dever fiduciário para com os clientes, e que os interesses comerciais - ou aqueles de seus clientes - não desviem o foco de seu trabalho.

[3] Bem como efetivos e consistentes com a natureza, complexidade e risco das operações realizadas para o exercício profissional de administração de carteiras de valores mobiliários.

(cinco) anos[4], os documentos e informações exigidos pela regulação aplicável[5].

1.6 Análise e Comunicação aos Órgãos Competentes

Toda desconformidade em temas de conduta pessoal e profissional - e a sua respectiva análise efetuada pelo *Compliance* - deve ser submetida ao Conselho de Ética da GESTORA para conclusão e deliberação dos passos a serem dados a tal respeito.

Nos casos aplicáveis de desvio da norma específica das atividades reguladas, o Diretor de *Compliance* deve comunicar os respectivos órgãos competentes, nos prazos regulatórios, como seguem:

a) A CVM deve ser comunicada no prazo máximo de 10 (dez) dias da verificação da respectiva ocorrência ou sua identificação, ou em prazo menor, se assim exigido pela regulação aplicável;

b) O COAF deve ser comunicado no prazo de 24 (vinte e quatro) horas da verificação da respectiva ocorrência ou sua identificação.

Os demais prazos aplicáveis à GESTORA encontram-se previstos no Anexo I a esta Política, bem como na planilha de controle interno detalhada, intitulada "Quadro de Rotinas".

1.7 Documentos de *Compliance* e Controles Internos

O Sistema de *Compliance* e Controles Internos da GESTORA está previsto em seus documentos internos, que englobam todas as suas políticas, manuais e Código de Ética e Conduta Profissional, além dos seguintes procedimentos e organismos:

1.7.1 Documentos Específicos Disponibilizados no *Website* da GESTORA

Cabe ao Diretor de *Compliance* preencher o respectivo Formulário de Referência da GESTORA e mantê-lo em seu *website*. Tal formulário deve ser atualizado obrigatoriamente até o dia 31 de março de cada ano.

Adicionalmente, cabe ao Diretor de *Compliance* manter no *website* da GESTORA, em suas versões atualizadas, os seguintes documentos:

a) Código de Ética e Conduta Profissional;

b) Formulário de Referência da GESTORA;

c) Política de Compliance e Controles Internos;

d) Política de Gestão de Riscos;

e) Política de Investimentos Pessoais e da Empresa;

f) Política de Rateio de Ordens de Investimento; e

[4] Ou prazo superior por determinação expressa da CVM.

[5] Bem como correspondência, interna e externa, papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções. Os documentos e informações podem ser guardados em meio físico ou eletrônico, admitindo-se a substituição de documentos originais por imagens digitalizadas.

g) Política de Exercício do Direito de Voto em Assembleias Gerais.

1.7.2 Teste e Relatório anual

Para verificação dos controles internos, sua efetividade e consistência com a natureza, complexidade e riscos das operações realizadas pela GESTORA, é realizado um teste anual de aderência, o qual deve ser formalizado em relatório[6].

O relatório é de responsabilidade do Diretor de *Compliance*, e, após ratificação pelo Comitê de *Compliance*, é encaminhado à alta administração da GESTORA anualmente, até o último dia útil de abril de cada ano[7].

O Relatório Anual fica disponível para consulta da CVM, na sede da GESTORA.

Tal relatório contém:

a) As conclusões dos exames efetuados relativos aos controles internos e *compliance*, inclusive o Teste Anual dos Sistemas de Informações - os testes periódicos dos sistemas de informações, em especial para os mantidos em meio eletrônico, efetuados pela Diretoria de *Compliance*[8];

b) As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e

c) A manifestação do Diretor de Investimentos, ou, quando for o caso, dos Diretores de Risco e de *Compliance* a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las.

1.8 Organismos Relacionados a *Compliance* e Controles Internos

1.8.1 Comitê de *Compliance*

O Comitê de *Compliance* é responsável por avaliar o descumprimento das normas legais, regulatórias, autorregulatórias e das políticas, manuais e procedimentos internos da GESTORA.

Ademais, cabe ao Comitê de *Compliance* avaliar, do ponto de vista normativo, a atividade da GESTORA e dos veículos de investimento sob sua responsabilidade, a fim de garantir a aderência à legislação e normas regulatórias e autorregulatórias em vigor, bem como aprovar ações de correção nestas matérias, além de:

a) Avaliar os processos internos da GESTORA do ponto de vista de melhores práticas, bem como avaliar as ocorrências do período;

b) Concluir por eventuais apontamentos de situações irregulares ao Conselho de Ética e/ou à alta administração da GESTORA;

c) Analisar eventuais situações ocorridas de desenquadramento de mandato no

[6] V. modelo no Anexo II, e orientação sobre o respectivo conteúdo no Anexo III.

[7] Com conteúdo relativo ao ano civil imediatamente anterior.

[8] Devem: (i) assegurar que os recursos humanos e computacionais estão adequados ao porte e à área de atuação da GESTORA, (ii) garantir o adequado nível de confidencialidade e acessos às informações confidenciais, (iii) assegurar que os recursos computacionais estão protegidos contra adulterações e (iv) assegurar que a manutenção de registros permite a realização de auditorias e inspeções.

mês anterior, procedimentos adotados, e recomendações de controle futuro;

d) Elaborar e distribuir a Lista Restrita de Ativos da GESTORA fazendo seu acompanhamento e monitoramento; e

e) Monitorar mudanças regulatórias e coordenar ajustes e adaptações necessárias na GESTORA e seus produtos.

Periodicidade: quadrimestral, sem prejuízo de reuniões extraordinárias, se aas circunstâncias assim demandarem.

Participantes: Diretores (sempre com a presença do Diretor de *Compliance*), e demais integrantes da Área de *Compliance.*

Convidados: podem ser convidados outros Colaboradores da GESTORA, porém sem direito a voto.

Quórum mínimo: Necessária a presença de ao menos três membros, sendo obrigatória a presença do Diretor de *Compliance* (ou representante por ele designado).

Formalização das decisões: atas do Comitê sob responsabilidade da Área de *Compliance.*

1.8.2 Comitê de Risco

O Comitê de Risco tem suas atribuições descritas na forma definida na Política de Gestão de Riscos da GESTORA.

1.8.3 Conselho de Ética

O Conselho de Ética tem suas atribuições descritas na forma definida no Código de Ética e Conduta Profissional da GESTORA.

1.9 Segregação de Atividades

Cabe ao Diretor de *Compliance* assegurar e verificar que sejam devidamente segregadas da atividade de gestão todas e quaisquer atividades eventualmente desempenhadas pela GESTORA, que com aquela guardem qualquer tipo de conflito, real ou potencial, em qualquer grau, aspecto, medida, tempo e/ou forma: a segregação em questão deverá se dar tanto física quanto logicamente, com restrição de acesso a dependências, sistemas, diretórios e arquivos apenas aos Colaboradores autorizados de cada área pertinente da GESTORA - e, se for o caso, entre estes e colaboradores de empresas de seu grupo econômico -, nos termos desta e das suas demais Políticas.

Todas e quaisquer atribuições de controle na GESTORA – notadamente, mas sem limitação, o próprio *compliance* e o gerenciamento de riscos – não depende nem está sujeito às suas áreas de negócios, de forma a assegurar a total autonomia de tais controles frente a cogitações de ordem comercial ou de gestão de carteiras de valores mobiliários.

1.10 Contratações Externas

A contratação de serviços de terceiros deve ser precedida das seguintes providências[9]:

a) Exigência de documentos e das certidões reputadas convenientes, seguindo, quando aplicável, procedimentos semelhantes aos descritos na Política de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Corrupção;

b) De acordo com a avaliação de conveniência dos profissionais envolvidos, solicitar a assinatura, pelos terceiros a serem contratados, de "Acordo de Não Divulgação" (*Non-Disclosure Agreement* ou "NDA"); e

c) Nos processos de negociação de qualquer contrato a ser celebrado pela GESTORA, o Colaborador envolvido na negociação deverá informar ao Comitê de *Compliance* sobre qualquer relacionamento familiar ou pessoal, sejam laços de amizade ou negocial, que tenha com membros do potencial contratado.

Após a contratação dos respectivos serviços, a área de *Compliance* da GESTORA poderá, a seu critério, supervisionar os contratados[10].

O processo para contratação de terceiros poderá vir acompanhado ou não de concorrência prévia, visando a obter o melhor "custo x benefício" dos melhores prestadores de serviço do mercado. Cabe à área responsável pela contratação definir ou não se será adotado este procedimento, sendo responsável inclusive por dar as devidas justificativas pelo "não uso", na hipótese de questionamento.

Qualquer eventual exceção às normas acima deverá ser reportada no Comitê de *Compliance*.

A contratação de terceiros deverá ser orientada pelas seguintes diretrizes:

a) O critério principal para escolha e contratação de terceiros será a modalidade menor preço, mediante a obtenção de orçamentos em número determinado pelo Diretor de *Compliance* para escolha do fornecedor ou prestador de serviços;

b) Em casos excepcionais em que um fornecedor mais caro seja escolhido, a contratação deverá ser justificada com os outros critérios (por exemplo: prazo, qualidade, *expertise*, menor impacto ambiental etc.);

c) Não haverá exigência de concorrência:

- Nas compras e contratações para valores inferiores a R$ 50.000,00 (cinquenta mil reais), desde que os pagamentos não se refiram a parcelas de um mesmo serviço;
- Quando houver prestação de serviços recorrentes, não sendo, neste caso, necessário realizar concorrência a cada contratação;

[9] O *Compliance* poderá demandar medidas adicionais pré-contratação, tais como visita às dependências do prestador de serviço, clippings de mídia impressa/internet, além de outras medidas reputadas cabíveis/convenientes à contratação.

[10] A supervisão poderá ser realizada mediante procedimentos diversos a critério do *Compliance*, tais como visitas in loco, clippings de mídia impressa/internet, requisição periódica de certidões administrativas/judiciais, além de outras medidas reputadas cabíveis/convenientes à contratação.

- Em compras e contratações para as quais houver fornecedor/prestador especializado;
- Em compras e contratações em casos emergenciais, caracterizados pela urgência de atendimento de situação que possa ocasionar prejuízo ou comprometer trabalhos, e que não pôde ser prevista antecipadamente.

1.11 Supervisão Baseada em Risco - SBR

A GESTORA adota metodologia própria de supervisão baseada em risco ("SBR"), mediante os seguintes critérios:

I – Alto Risco: são considerados de "alto risco" os prestadores de serviço que, individual ou cumulativamente:

a) Tenham quaisquer apontamentos verificados no processo de pré-contratação da GESTORA, sem oferecer, ou tendo se recusado a dar, justificativa para as ocorrências constatadas;

b) Não estejam em dia com as suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou com suas obrigações autorregulatórias, quando aplicáveis;

c) Tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores, sem oferecer, ou tendo se recusado a dar, as devidas explicações para tanto;

d) Tenham apontamentos verificados no processo de screening da GESTORA, via mídia impressa ou na internet, sem justificativa plausível para tal;

e) Movimentem, sem embasamento econômico-financeiro plausível, somas superiores a R$ 100.000,00 (cem mil reais);

f) Se recusem a permitir o acesso de Colaboradores do Jurídico/*Compliance* da GESTORA às suas dependências, quando do procedimento de pós-contratação;

g) Tenham, em seus quadros Pessoas Politicamente Expostas, conforme definidas na Política de *Compliance* da GESTORA;

h) Falhem em atender, sem justificativa, outros critérios reputados convenientes pela GESTORA na verificação de suas atividades/idoneidade;

II – Médio Risco: são considerados de "médio risco" os prestadores de serviço que, individual ou cumulativamente:

a) Tenham apontamentos verificados no processo de pré-contratação da GESTORA, oferecendo, porém, justificativa plausível para tanto;

b) Estejam em processo de regularização de suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou de suas obrigações autorregulatórias, quando aplicáveis;

c) Tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores, oferecendo, porém, as devidas explicações para tanto;

d) Tenham apontamentos verificados no processo de screening da GESTORA,

via mídia impressa ou na internet, justificando a contento da GESTORA a ocorrência verificada;

e) Movimentem, mediante as competentes explicações e justificativas, somas superiores a R$ 100.000,00 (cem mil reais);

f) Falhem em atender, mas remediando posteriormente, outros critérios reputados convenientes pela GESTORA na verificação de suas atividades/idoneidade;

III – Baixo Risco: são considerados de "baixo risco" os prestadores de serviço que:

a) Não tenham quaisquer apontamentos verificados no processo de pré-contratação da GESTORA;

b) Estejam em dia com as suas eventuais obrigações regulatórias junto aos órgãos competentes, e/ou com suas obrigações autorregulatórias, quando aplicáveis;

c) Não tenham apontamentos judiciais ou administrativos em seus nomes, ou de qualquer de seus sócios, administradores ou colaboradores;

d) Não tenham apontamentos verificados no processo de screening da GESTORA, via mídia impressa ou na internet, sem justificativa plausível para tal;

e) Tenham pleno embasamento movimentar somas superiores a R$ 100.000,00 (cem mil reais);

f) Atendam, com sucesso, outros critérios reputados convenientes pela GESTORA na verificação de suas atividades/idoneidade.

A SBR será feita pela GESTORA mediante os seguintes termos e periodicidade:

I – Alto Risco: a SBR dos fornecedores/prestadores de serviço de "alto risco" engloba os seguintes procedimentos:

a) Acompanhamento periódico mensal via pesquisas em sites de Tribunais de Justiça para verificação de eventuais processos judiciais, além de requisição de certidões administrativas online e clipping de notícias/internet;

b) Requisição de inspeções in loco sem ciência prévia do fornecedor/prestador de serviço;

c) Requisição de informações adicionais no dossiê de due diligence do fornecedor/prestador de serviço sempre que reputado necessário;

d) Avaliação do fornecedor/prestador de serviço a cada 12 (doze) meses, ou em periodicidade menor, se assim considerado necessário;

e) Na ocorrência de qualquer fato novo que justifique a respectiva reclassificação do fornecedor/prestador de serviço, o *Compliance* da GESTORA procederá às medidas aplicáveis em até 72 (setenta e duas) horas úteis.

II – Médio Risco: a supervisão dos fornecedores/prestadores de serviço de "médio risco" engloba os seguintes procedimentos:

a) Acompanhamento periódico trimestral via pesquisas em sites de Tribunais de Justiça para verificação de eventuais processos judiciais, além de requisição

de certidões administrativas online e clipping de notícias/internet na mesma periodicidade;

b) Requisição de inspeções in loco mediante ciência prévia do fornecedor/prestador de serviço;

c) Requisição de informações adicionais no dossiê de due diligence do fornecedor/prestador de serviço sempre que reputado necessário;

d) Avaliação do fornecedor/prestador de serviço a cada 12 (doze) meses;

e) Na ocorrência de qualquer fato novo que justifique a respectiva reclassificação do fornecedor/prestador de serviço, o *Compliance* da GESTORA procederá às medidas aplicáveis em até 72 (setenta e duas) horas úteis.

III – Baixo Risco: a SBR dos fornecedores/prestadores de serviço de "baixo risco" engloba os seguintes procedimentos:

a) Acompanhamento periódico semestral via pesquisas em sites de Tribunais de Justiça para verificação de eventuais processos judiciais, além de requisição de certidões administrativas online e clipping de notícias/internet na mesma periodicidade;

b) Inspeções in loco a cada 24 (vinte e quatro) meses, com ciência prévia do fornecedor/prestador de serviço;

c) Requisição de informações adicionais no dossiê de due diligence do fornecedor/prestador de serviço sempre que reputado necessário;

d) Avaliação do fornecedor/prestador de serviço a cada 24 (vinte e quatro) meses;

e) Na ocorrência de qualquer fato novo que justifique a respectiva reclassificação do fornecedor/prestador de serviço, o *Compliance* da GESTORA procederá às medidas aplicáveis em até 72 (setenta e duas) horas úteis.

1.12 Soft Dollar

A prática de *soft dollar* é vedada na GESTORA, salvo exceções expressas e circunstanciadas pelo Diretor de *Compliance*, e apenas se comprovada a conveniência da ferramenta permutada na eficiência da gestão de fundos e carteiras a cargo da GESTORA.

2. Política de Certificação

2.1 A quem se aplica?

Sócios, diretores e funcionários da MAXIPLAN LTDA. ("GESTORA"), que desempenhem atividades diretas de gestão profissional de carteiras de títulos e valores mobiliários, com alçada de decisão sobre o investimento, desinvestimento e manutenção dos recursos dos veículos a cargo da GESTORA ("Colaboradores").

Assim sendo, a GESTORA requer dos profissionais elencados acima a "Certificação de Gestores ANBIMA" (CGA), sempre que aplicável às suas atividades.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de *Compliance*.

2.2 Responsabilidades

O **Diretor de *Compliance*** é responsável pelos controles que garantem o atendimento às demandas relativas à necessidade ou não de certificação dos profissionais da GESTORA.

2.3 Revisão e Atualização

Esta política deverá ser revisada a atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/ regulatórias/ autorregulatórias.

2.4 Controles

O Diretor de *Compliance* mantém controle dos Colaboradores da GESTORA com as seguintes informações:

a) Dados profissionais;

b) Data de admissão;

c) Data de desligamento, quando aplicável;

d) Atividade exercida;

e) Área de atuação;

f) Cargo;

g) Tipo de gestor, quando aplicável;

h) Endereço eletrônico individual;

i) Se dispõe de certificação ANBIMA e a sua validade.

O Diretor de *Compliance* é responsável por verificar que todos os Colaboradores elegíveis à CGA sejam certificados e que as respectivas certificações estejam válidas.

A CGA é válida por prazo indeterminado, desde que o profissional esteja exercendo atividades que dela sejam objeto.

Compete ao Diretor de *Compliance* garantir que um Colaborador não certificado não exerça função que pressuponha certificação ou que a obtenha nos termos ditados pela ANBIMA.

Caso o Colaborador não disponha da certificação aplicável, a Diretoria de *Compliance* é responsável por manter a documentação formal que evidencie o afastamento do Colaborador das atividades elegíveis à certificação.

Cabe ao Diretor de *Compliance* monitorar o cumprimento das demais diretrizes estabelecidas no Código de Certificação.

As certificações pendentes e o afastamento das funções elegíveis devem ser reportadas ao Comitê de *Compliance,* que deve monitorar a sua devida regularização.

Quaisquer outras situações identificadas aplicáveis à matéria devem ser objeto de análise, aprovação, formalização ou eventual assunção de risco no âmbito do Comitê de *Compliance.*

2.5 Admissões de Colaboradores

O Diretor de *Compliance* deve acompanhar as informações sobre novas admissões e transferências internas, e se os novos Colaboradores possuem a respectiva certificação ANBIMA eventualmente aplicável.

Os candidatos a cargos que pressupõem certificação CGA devem ser contratados com certificações válidas. Eventuais exceções deverão ser avaliadas pelo Diretor de *Compliance* e reportadas ao Comitê de *Compliance* para controle das respectivas atividades e possível afastamento das funções até a efetiva obtenção da certificação aplicável.

Compete à Área de *Compliance* cadastrar, no site da ANBIMA, o novo funcionário e/ou colaborador transferido internamente, o que deve ocorrer no mesmo mês da contratação/ transferência. Além disso, deve manter sempre atualizados os seus controles internos

2.6 Licenças e Desligamentos

No caso de licenças e desligamentos, o Diretor de *Compliance* deve verificar se o Colaborador está vinculado à GESTORA no site da ANBIMA, e, nesse caso, desvincular o profissional, o que deve ocorrer impreterivelmente no mesmo mês de licença e/ou desligamento.

Os profissionais em licença não devem continuar vinculados no período em que estiverem de licença. Quando retornarem, deverá ser efetuado o vínculo novamente.

2.7 Banco de Dados da ANBIMA

O Diretor de *Compliance* é responsável pela veracidade e manutenção do banco de dados da ANBIMA atualizado.

O controle de admissão, licença e demissão consta na agenda regulatória do Comitê de *Compliance*, onde são formalizados tais registros, devendo as eventuais atualizações junto à entidade ocorrer até o último dia do mês subsequente ao evento.

2.8 Código de Ética e Conduta Profissional

Cabe ao Diretor de *Compliance* requerer dos novos Colaboradores a assinatura formal do Termo de Conhecimento e Adesão ao Código de Ética e Conduta Profissional e das demais políticas da GESTORA, até o último dia do mês subsequente à sua contratação.

3. Política de Confidencialidade, Segurança da Informação e Cybersegurança

3.1 Objetivo

Estabelecer princípios e diretrizes de proteção das informações no âmbito da MAXIPLAN LTDA. (“GESTORA”).

3.2 A quem se aplica?

Sócios, diretores, funcionários, prestadores de serviço, terceirizados, consultores e

demais pessoas físicas ou jurídicas contratadas ou outras entidades, que participem, de forma direta, das atividades diárias e negócios, representando a GESTORA (doravante, "Colaboradores").

3.3 Responsabilidades

Os Colaboradores devem atender aos procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao Diretor de *Compliance*, que deverá avaliá-las e submetê-las ao Comitê de *Compliance* e/ou Conselho de Ética, conforme o caso.

O Diretor de *Compliance* deve garantir o atendimento a esta Política, sendo o responsável na GESTORA por temas de segurança da informação/cibernética.

3.4 Revisão e Atualização

Esta política deverá ser revisada a atualizada a cada 2 (dois) anos, ou em prazo inferior, caso necessário em virtude de mudanças legais/ regulatórias/ autorregulatórias.

3.5 Informações Confidenciais

São consideradas "Informações Confidenciais" aquelas não disponíveis ao público, que:

a) Identifiquem dados pessoais ou patrimoniais (da GESTORA ou de clientes);

b) Sejam objeto de acordo de confidencialidade celebrado com terceiros;

c) Identifiquem ações estratégicas – dos negócios da GESTORA, seus clientes ou dos portfólios sob gestão[11];

d) Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da GESTORA, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;

e) Sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória; e que

f) O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás), que são de uso pessoal e intransferível.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais: (i) mediante prévia autorização do Diretor de *Compliance*, (ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, bem como (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

3.6 Disposições Gerais

Os seguintes princípios norteiam a segurança da informação na GESTORA:

[11] Cuja divulgação possa prejudicar a gestão dos negócios, clientes e portfólios a cargo da GESTORA, ou reduzir sua vantagem competitiva.

a) Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando for de fato necessário;

b) Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

c) Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da GESTORA:

a) As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;

b) A informação deve ser utilizada apenas para os fins sob os quais foi coletada;

c) A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;

d) A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;

e) Segregação de instalações, equipamentos e informações comuns, quando aplicável;

f) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação deve ser reportado ao Diretor de *Compliance*.

3.7 Identificação, Classificação e Controle da Informação

O Colaborador que recebe ou prepara uma informação deve identificar a sua natureza. Algumas informações podem ser classificadas como “Confidenciais”.

Para tal, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

O acesso às Informações Confidenciais deve ser restrito e controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do Diretor de *Compliance*, e, se reputado necessário, da assessoria jurídica da GESTORA.

A informação deve receber proteção adequada. Em caso de dúvida, o Colaborador deverá consultar o Diretor de *Compliance*.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando preferencialmente máquina fragmentadora/trituradora de papéis ou incineradora.

3.8 Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

3.9 Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na GESTORA são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares, mediante autorização prévia do Diretor de *Compliance*.

A GESTORA poderá, a qualquer momento, mediante prévia aprovação do Diretor de *Compliance,* e SEM obrigação de cientificação prévia:

a) Inspecionar conteúdo e registrar o tipo de uso dos e-mails feitos pelos usuários;

b) Disponibilizar esses recursos a terceiros, caso entenda necessário;

c) Solicitar aos usuários justificativas pelo uso efetuado.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é imediatamente adaptada para compatibilizar/adequar o acesso, ou cancelada em definitivo, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

O Diretor de *Compliance* pode definir bloqueio a sites caso necessário. O monitoramento pode ser feito sem necessidade de prévia ciência dos Colaboradores.

O acesso a sites de armazenamento de arquivos em "nuvem" é permitido.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à GESTORA.

Apenas os Colaboradores devidamente autorizados terão acesso[12] às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da GESTORA, mediante segregação física e lógica.

3.10 Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e *Backups*

Os riscos e incidentes de segurança da informação devem ser reportados ao Diretor de *Compliance*, que adotará as medidas cabíveis.

O plano de contingência e de continuidade dos principais sistemas e serviços deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de *Compliance* deverá ser imediatamente comunicado, para a tomada das medidas cabíveis[13].

[12] Quaisquer exceções deverão ser previamente solicitadas ao Diretor de *Compliance*.

[13] Podendo variar de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada (para que apague em definitivo o seu conteúdo), até o estudo e implementação efetiva de providências judiciais, quando e se for o caso, sem prejuízo da investigação e eventual punição dos Colaboradores envolvidos.

3.11 Testes de Controles

A efetividade desta Política é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de *Compliance* e reportados ao Comitê de *Compliance*.

Os testes devem verificar se:

- Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;
- Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- Há segregação física e lógica;
- Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;
- A manutenção de registros permite a realização de auditorias e inspeções.

3.12 Riscos de Cybersegurança

As principais ameaças e riscos aos ativos cibernéticos da GESTORA são:

a) *Malwares* – *softwares* desenvolvidos para corromper os computadores e redes, como:

- vírus: *software* que causa danos às máquinas, redes, *softwares* e bancos de dados;
- cavalos de troia: aparecem dentro de outro *software*, criando uma entrada para invasão da máquina;
- *spywares*: *softwares* maliciosos que coletam e monitoram as atividades das máquinas invadidas;
- *ransomware*: *softwares* maliciosos que bloqueiam o acesso a sistemas e bases de dados, solicitando resgates para restabelecimento do uso/acesso.

b) *Engenharia social – métodos de manipulação para obter informações* confidenciais, como senhas, dados pessoais e número de cartão de crédito, como, por exemplo:

- *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
- *phishing*: *links* veiculados por e-mails simulando pessoas ou empresas confiáveis que enviam comunicação eletrônica aparentemente oficial para obter informações confidenciais;
- *vishing*: simulação de pessoas ou empresas confiáveis para, por meio de ligações telefônicas, obtenção de informações confidenciais;
- *smishing*: simulação de pessoas ou empresas confiáveis para, por meio de mensagens de texto, obtenção de informações confidenciais;
- ataques de DDOS (*distributed denial of services*) e *botnets* – ataques visando a negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

3.13 Obrigações de Cybersegurança

Na prestação de seus serviços, a GESTORA obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos[14].

O responsável por tais questões na GESTORA é o **Diretor de *Compliance***.

São itens obrigatórios de Cybersergurança (empresa):

a) A adequada proteção dos ativos cibernéticos da GESTORA, aí incluídos sua rede, sistemas, *softwares*, websites, equipamentos e arquivos eletrônicos.;

b) Restrição e controle do acesso e privilégios de usuários remotos e externos;

c) Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;

d) Quando necessário, bloquear chaves de acesso de usuários, e, quando necessário, realizar auditoria para verificação de acessos indevidos;

e) Excluir ou desabilitar contas inativas;

f) Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;

g) Garantir o cumprimento do procedimento de *backup* para os servidores e ativos cibernéticos, eletrônicos e computacionais da GESTORA;

h) Detectar, identificar, registrar e comunicar ao Diretor de *Compliance* as violações ou tentativas de acesso não autorizadas;

i) Organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário;

j) Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;

k) Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;

l) A GESTORA dispõe de *firewall* de segurança nos servidores para acesso à sua rede, visando a manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado;

m) É realizado backup de arquivos de forma sistemática. Os dados de backup atualizados são armazenados em local seguro, com monitoramento.

São itens obrigatórios de cybersergurança (Colaboradores):

a) Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;

b) Somente imprimir as mensagens quando realmente necessário;

c) Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a

[14] Os riscos potenciais relativos a tais dados envolvem invasões, disseminação errônea ou dolosa, acesso indevido e/ou seu roubo/desvio.

segurança em abrí-la, para evitar vírus ou códigos maliciosos;

d) No caso de recebimento de mensagens que contrariem as regras estabelecidas pela GESTORA, NUNCA as repassar, alertando o responsável da sua área e o Diretor de Compliance, se for o caso;

e) Ao se ausentar do seu local de trabalho, mesmo que temporariamente, bloquear a estação de trabalho;

f) Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;

g) Utilizar equipamentos, aplicativos, impressoras, acesso a sites, e e-mail (e demais ferramentas tecnológicas) com a finalidade primordial de atender aos interesses da GESTORA[15];

h) É permitido o uso pessoal (de forma moderada) dos equipamentos de informática e de comunicação de propriedade da GESTORA, sempre lembrando que pertencem à GESTORA e são rastreáveis e sujeitos a monitoramento;[16]

i) Tecnologias, marcas, metodologias e quaisquer informações que pertençam à GESTORA não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho;

j) A gravação de cópias de arquivos e instalação de programas em computadores deverá ser previamente autorizada pelo responsável pelo departamento da GESTORA;

k) Em regra, os acessos a dispositivos móveis, como pen drives, HDs externos, cartões de memória, estão bloqueados na GESTORA, devendo as eventuais exceções devem ser previamente aprovadas pelo responsável pelo *Compliance*;

l) Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

São itens VEDADOS de cybersergurança (Colaboradores):

a) Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais[17];

b) Divulgar informações ou trocar arquivos com configurações dos equipamentos e de negócios da GESTORA, ou qualquer outra informação sobre a GESTORA, seus negócios, clientes, produtos, equipamentos ou Colaboradores, sem prévia aprovação[18];

c) Trocar informações que causem quebra de sigilo bancário e/ou possuam

[15] Os computadores, arquivos, e, arquivos de e-mails corporativos poderão ser inspecionados, independentemente de prévia notificação ao Colaborador, a fim de disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações;

[16] Sem a necessidade de ciência prévia do Colaborador, bem como podem se tornar públicos em caso de auditoria, exigência judicial ou regulatória.

[17] Sendo proibido, sobretudo, conteúdo pornográfico, racista ou ofensivo à moral e aos princípios éticos.

[18] Em caso de exigência de alguma autoridade ou entidade autorreguladora, o Colaborador deverá solicitar orientação ao Diretor de *Compliance*.

caráter confidencial ou estratégico;

d) Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da GESTORA;

e) Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da GESTORA;

f) Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo Diretor de *Compliance*;

g) Contratar provedores de acesso sem autorização prévia do Diretor de *Compliance*;

h) Redirecionar caixa postal pessoal (e-mail de outros provedores) para a sua caixa postal de correio eletrônico na GESTORA e vice-versa.

i) Uso de compartilhadores de informações, tais como redes *Peer-toPeer* (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da GESTORA;

j) *Download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura da GESTORA ou que violem direitos autorais.

ANEXO I

Quadro de Obrigações Periódicas da GESTORA

I - Informações Periódicas

Norma	Artigo	Tema	Obrigação	Período
ICVM 558	22, *caput*	Relatório Anual	Entrega do relatório à administração da GESTORA	Último dia útil de abril a cada ano (Data base 31/12)
ICVM 558	15, *caput*, I e II	Formulário de Referência	Envio do FR pelo CVMWeb	Anualmente, até 31/03 (Data base 31/12)
ICVM 510	1.º, II	Declaração Eletrônica de Conformidade	Envio pelo CVMWeb	Anualmente, até 31/03 (Data base 31/12)
ICVM 301	3.º, § 2.º	Política de PLD	Atualização dos dados cadastrais dos clientes/investidores e/ou verificação da efetiva atualização dos citados dados pelo administrador/distribuidor	No máximo a cada 24 (vinte e quatro) meses
ICVM 301	7.º - A, *caput*	Política de PLD	Declaração Negativa através da CVMWeb à CVM ou ao órgão que esta indicar, desde que não tenha sido prestada nenhuma comunicação durante exercício anterior ao COAF acerca de operações ou propostas de operações com indícios de lavagem de dinheiro	Anualmente, até o último dia útil do mês de janeiro
Código Certificação ANBIMA	23, § 2.º	Base de Dados ANBIMA	Inclusão e atualização no banco de dados administrado pela ANBIMA das informações relativas aos colaboradores certificados, em processo de certificação, com a certificação vencida, e/ou em processo de atualização da certificação	Mensalmente, até o último dia do mês subsequente à data do evento

II - Informações Eventuais

Norma	Artigo	Tema	Obrigação	Período
ICVM 510	1.º, I	Atualização de dados cadastrais	Atualização via CVMWeb	7 (sete) dias úteis contados do evento que deu causa à alteração
ICVM 301	7.º, *caput*, I e II	Política de PLD	Comunicar ao COAF todas as transações, ou propostas de transação, que possam ser consideradas sérios indícios de crimes de lavagem ou ocultação de bens, direitos e valores provenientes de infração penal	24 (vinte e quatro) horas a contar da ocorrência
ICVM 558	16, VIII	Violação à regulação	Informar à CVM a ocorrência ou indícios de violação da sua regulação	10 (dez) dias úteis da ocorrência ou sua identificação
Ofício Circular CVM/SIN 10/15	Item 37	Atualização cadastral	Envio à CVM do contrato social atualizado, no caso de mudança de denominação social ou de substituição de diretor responsável pela gestão	7 (sete) dias úteis do fato que deu causa à alteração

ANEXO II

Modelo de Relatório de Aderência

Ilmos. Srs.

Sócios e Diretores da

[GESTORA]

Ref.: Relatório Anual – Instrução CVM nº 558, de [ano]

Prezados Senhores,

Em cumprimento ao disposto no art. 22 da Instrução CVM n.º 558, de 26 de março de 2015 ("ICVM 558"), vimos apresentar a V.Sas. o relatório pertinente às atividades da **MAXIPLAN LTDA.**, ("GESTORA") no ano de [•] ("Relatório").

De acordo com a ICVM 558, o mencionado Relatório contém:

a) As conclusões dos exames efetuados;
b) As recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e
c) A manifestação do diretor responsável pela administração de carteiras de valores mobiliários, ou, quando for o caso, pelo diretor responsável pela gestão de risco, a respeito das eventuais deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las (cf. art. 22, I, II e III, da ICVM 558).

Este relatório ficará à disposição da Comissão de Valores Mobiliários ("CVM") na sede da GESTORA, para eventuais posteriores checagens, verificações e/ou fiscalizações por parte da CVM.

Além dos aspectos acima, V.Sas. encontrarão também, no corpo do presente Relatório, os resultados do Teste de Aderência determinado na Política de *Compliance* e Controles Internos da GESTORA, e o correspondente parecer final do Diretor *Compliance* e Controles Internos, que assina o presente documento.

Assim sendo, passamos abaixo à exposição dos elementos pertinentes do presente Relatório.

1. Conclusão dos Exames Efetuados (ICVM 558, art. 22, I)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo datas da verificação da ocorrência e sua natureza)

2. Recomendações sobre as Deficiências Encontradas e Cronogramas de Saneamento (ICVM 558, art. 22, II)

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo estimativas de datas de acompanhamento e conclusão das soluções)

3. <u>Manifestações dos Diretores Correspondentes de Gestão e de Risco sobre as Verificações Anteriores e Respectivas Medidas Planejadas (ICVM 558, art. 22, III)</u>

(enumerar detalhadamente por área/ocorrência, com todas as informações pertinentes, incluindo os resultados esperados e os efetivamente alcançados)

4. <u>Parecer Final do Diretor de Risco, *Compliance* e Controles Internos</u>

(enumerar detalhadamente)

Sendo então o que nos cumpria para o momento, aproveitamos o ensejo desta correspondência para nos colocarmos à disposição de V.Sas. para os eventuais esclarecimentos porventura reputados necessários.

Atenciosamente,

[•]

[GESTORA]

Diretor de *Compliance* e Controles Interno

ANEXO III

Organograma Funcional da Maxiplan Ltda.