REGRAS, PROCEDIMENTOS E DESCRIÇÃO DE CONTROLES INTERNOS

1. Objetivo e Abrangência

Este manual de Regras, Procedimentos e Descrição de Controles Internos da Fornax Assessoria Ltda. ("Manual" e "Gestor") está de acordo com os termos da Resolução CVM 21, de 25 de fevereiro de 2021 ("Resolução CVM 21"), e é aplicável a todos os sócios, Diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando o Gestor ("Colaboradores"), devendo ser aplicado em conjunto com o Manual de Segregação de Atividades e Segurança da Informação e com as demais normas e políticas do Gestor.

Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos neste Manual, informando qualquer irregularidade à Diretoria de *Compliance* e Riscos, de modo que sejam alcançados os objetivos abaixo:

(i) estabelecer uma estrutura para possibilitar que os Colaboradores atuem com imparcialidade, tenham conhecimento do Código de Ética, a legislação e regulamentação aplicável, bem como as demais políticas internas do Gestor;

(ii) monitorar a adequação do Gestor e de seus Colaboradores a esta estrutura, para identificar, administrar e eliminar eventuais conflitos de interesses que possam afetar a imparcialidade dos Colaboradores ligados à área de gestão; e

(iii) prevenir, controlar e mitigar os riscos envolvidos nas atividades desenvolvidas pelo Gestor.

2. Estrutura Organizacional

O Gestor será administrado por uma *Diretoria*, composta por 02 (dois) Diretores, a serem designados no Contrato Social, para atuar por prazo indeterminado. A Diretoria de Gestão será responsável pela administração de carteiras de valores mobiliários, nos termos da Resolução CVM 21, enquanto a Diretoria de *Compliance* e Riscos ficará responsável (a) pelo cumprimento de regras, políticas, procedimentos e controles internos e da Resolução CVM 21, (b) pela gestão de risco, e (c) pelo cumprimento das obrigações estabelecidas na Resolução CVM 50, de 31 de agosto de 2021 ("Resolução CVM 50"), relativas à prevenção da lavagem de dinheiro e ao financiamento ao terrorismo ("PLDFT").

O *Departamento Técnico* será formado pelo Diretor de Gestão e será responsável por tomar as decisões de investimento e desinvestimento - definição de estratégias, originação e decisão de investimentos, formas de criação de valor nas investidas - e pelo monitoramento diariamente das operações da investida do fundo de investimento sob gestão, devendo auxiliar também os projetos de integração dos investimentos mais recentes ao portifólio.

As decisões de investimento e de desinvestimento serão tomadas pela Diretoria de Gestão e os documentos e informações que as fundamentarem deverão ser arquivados em meio eletrônico e passíveis de verificação. Quando for o caso, além das deliberações e da decisão tomada, as atas poderão fazer menção aos documentos que auxiliaram e que fundamentaram as decisões tomadas.

Apesar das atribuições usuais acima, cumpre ao Gestor esclarecer que, atualmente, faz a gestão de apenas um fundo de investimento em participações, em fase final de desinvestimento e com apenas um ativo na carteira, qual seja, ações de emissão de companhia fechada habilitada em rol de credores de um processo de falência. Em vista do exposto acima, o Gestor destaca que se mantem em atividade apenas em decorrência do dever fiduciário assumido com os investidores.

A área de *Compliance, Riscos e PLDFT* será composta por 01 (um) colaborador, o Diretor de *Compliance* e Riscos. A área será responsável pelo cumprimento de regras, políticas, procedimentos, controles internos, pela gestão de risco e pelo cumprimento das obrigações

estabelecidas na Resolução CVM 50, relativas à prevenção da lavagem de dinheiro e financiamento ao terrorismo. Sem prejuízo, o Diretor ficará também responsável (i) pelas atividades de natureza financeira e administrativa da organização; e (ii) pela supervisão dos prestadores de serviço responsáveis pela área de tecnologia da informação, contabilidade, assessoria jurídica e outros contratados em base *ad hoc*.

Os prestadores de serviço de tecnologia da informação – item (ii), supra - serão responsáveis pela implantação e racionalização de processos, manutenção dos sistemas de informática, segurança da informação com controle de acesso dos usuários. O *backup* de dados é integrado no *Office 365 Business Standard*.

A área de *Compliance*, Riscos e PLDFT contará ainda com prestadores de serviço terceirizados para as áreas jurídica, contábil, de tecnologia da informação, recursos humanos, guarda de documentos, tesouraria e serviços gerais.

2.1. Descrição dos Controles Internos

Visando garantir a mensuração e o alcance dos objetivos deste Manual, o Gestor implementará controles internos, conforme ou similares ao rol exemplificativo abaixo:

Segurança da Informação – o Gestor atuará por meio de rotinas elaboradas por prestadores de serviço especializados para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores, evitando que a qualidade da gestão seja afetada por contingências;

Monitoramento de E-mails - o Gestor terá equipamentos atualizados e seu servidor de e-mails será hospedado junto a Microsoft, através do plano Microsoft Office 365 Business Standard, do *Exchange Online*, o que garantirá alta disponibilidade e segurança e viabilizará o trabalho remoto e via computadores reserva, se e quando necessário, sem prejuízo da manutenção de registros que irão viabilizar a realização de auditorias e inspeções;

Identidade dos Colaboradores – a administração ocorrerá de forma centralizada através de servidor, onde (i) usuários e suas atividades podem ser monitorados; (ii) o particionamento das pastas é viabilizado; e (iii) os perfis de acesso são configurados conforme as prerrogativas e necessidades inerentes aos cargos dos colaboradores;

Telefonia - PABX com canais na sala de gestão, linha exclusiva para uso de fax e linhas móveis corporativas como meios de comunicação;

Aspectos Contratuais – a efetiva celebração de quaisquer contratos e acordos pelo Gestor será precedida de (i) validação pelos assessores jurídicos contratados; (ii) verificação de poderes de representação; (ii) alinhamento de trâmites de assinatura – eletrônica sempre que possível -; e (iii) arquivamento das versões assinadas, com controle de prazos centralizado; e

Contratação de Prestadores de Serviço - a efetiva contratação de novos Colaboradores ou prestadores de serviço para o Gestor (ou para o FIP, quando aplicável), bem como bem como a aprovação de profissionais para compor a administração da sociedade investida do FIP, será precedida de *background checks* e/ou due diligence específica, visando identificar o grau de risco apresentado pelo potencial contratado e o estabelecimento de critérios para acompanhamento de suas atribuições (contratuais ou não).

Fazemos referência à Política de Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo ("Política de PLDFT"), que traz, como anexo, o Manual de *Know Your Client*, *Know Your Partner*, e *Know Your Employee* ("KYC", "KYP", "KYE" e "Manual de ID", respectivamente), do Gestor para informações adicionais sobre os Controles Internos.

3. Responsabilidades e Reporte às Autoridades Competentes

O acompanhamento e a responsabilidade pelo cumprimento das disposições do presente Manual serão da Diretoria de *Compliance* e Riscos, que, visando alcançar os objetivos listados no item 1 acima e assegurar a existência de controles internos adequados, deverá:

(i) desenvolver e manter procedimentos para garantir que as atividades do Gestor respeitem as exigências legais e regulatórias, avaliando a adequação, abrangência e efetividade dos sistemas de *Compliance* e controles internos;

(ii) estabelecer um plano de continuidade para recuperação de dados ou interrupções periódicas dos mercados financeiros, bem como garantir que sejam realizados testes periódicos de segurança;

(iii) fiscalizar os serviços prestados por terceiros contratados por meio de controle contratual e avaliação de qualidade;

(iv) contratar consultores específicos para realização de "*background checks*" de parceiros, mantendo arquivados os relatórios recebidos;

(v) consolidar as comunicações entre o Gestor e os órgãos reguladores e autorreguladores.

Adicionalmente, nos termos do artigo 25 da Resolução CVM 21, será dever da Diretoria de *Compliance* e Riscos, encaminhar aos órgãos de administração do Gestor, até o último dia útil do mês de abril de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (a) as conclusões dos exames efetuados conforme acima; (b) as recomendações de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (c) a manifestação do Diretor(a) responsável pela administração de carteiras de valores mobiliários ou, quando for o caso, do Diretor(a) a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las ("Relatório Anual de Compliance").

Por fim, em conjunto com o Relatório Anual de Compliance, a Diretoria de *Compliance* e Riscos deverá elaborar relatório relativo à avaliação interna de PLDFT, a ser encaminhado para os órgãos da alta administração especificados na política de PLDFT[1].

4. Segregação da Atividade de Gestão

Fazemos referência ao Manual de Segregação de Atividades e Segurança da Informação para maiores informações com relação a este tema.

5. Confidencialidade e Sigilo

Informações Confidenciais:

No exercício de suas atividades, os Colaboradores poderão ter acesso a informações de clientes do Gestor, bem como de terceiros, que não sejam de conhecimento do público em geral e que,

[1] Contendo (a) a lista de todos os produtos oferecidos, serviços prestados, respectivos canais de distribuição e ambientes de negociação e registro em que o Gestor atue, classificados confirme Avaliação Interna de Risco ("AIR"); (b) a classificação dos clientes do Gestor, nos termos da AIR; (c) identificação e análise das situações de risco de LD/FTP, considerando as respectivas ameaças, vulnerabilidades e consequências; (d) se for o caso, análise da atuação dos prepostos ou prestadores de serviços relevantes contratados, bem como a descrição da governança e dos deveres associados à manutenção do cadastro simplificado previsto na Resolução CVM 50; (e) tabela relativa ao ano anterior, contendo: o número consolidado das operações e situações atípicas detectadas, segregadas por cada hipótese; o número de análises realizadas; o número de comunicações de operações suspeitas reportadas para o Conselho de Controle de Atividades Financeiras – COAF ou a data do reporte da declaração negativa; as medidas adotadas para a tratar e mitigar os riscos identificados (inclusive com a apresentação dos indicadores de efetividade nos termos definidos na política de PLDFT), incluindo a tempestividade acerca das atividades de detecção, análise e comunicação de operações ou situações atípicas; e a apresentação, se for o caso, de recomendações visando mitigar os riscos identificados do exercício anterior que ainda não foram devidamente tratados.

portanto, possam ser consideradas confidenciais ("Informações Confidenciais" ou, no singular, "Informação Confidencial"). É terminantemente proibida a divulgação de qualquer Informação Confidencial para terceiros, para benefício próprio ou de terceiro (*tipping*), ou mesmo que não haja intenção de beneficiar ninguém. A obrigação de confidencialidade se aplica mesmo após o desligamento do Colaborador.

O Gestor e Colaboradores possuem o dever legal e profissional de manter o sigilo quanto às Informações Confidenciais de seus clientes, de modo que pedidos, tentativas ou ações visando a quebra do sigilo deverão ser imediatamente comunicados à Diretoria de *Compliance* e Riscos, para que decidam quanto à sua regularidade e necessidade.

Informações Sigilosas:

Informações Sigilosas, além das Informações Confidenciais, são aquelas que, caso venham à tona, podem resultar em perda do nível de segurança do Gestor.

Perda, mau uso, modificação ou acesso não autorizado às Informações Sigilosas podem afetar adversamente a privacidade de um indivíduo, desfazer negócios, macular a imagem do Gestor e a continuidade de seus negócios.

O Gestor tem a responsabilidade legal de prezar pelo sigilo de seus clientes e, portanto, informações relativas aos clientes e entidades investidas por fundos de investimento geridos pelo Gestor jamais poderão ser enviadas a terceiros, com exceção das solicitações dos órgãos públicos, dos órgãos reguladores e do Poder Judiciário e, mesmo nessas hipóteses, nos estritos limites das ordens recebidas.

A divulgação e acesso às Informações Confidenciais e às Informações Sigilosas devem ser feitos apenas aos Colaboradores que venham a auxiliar e participar do desenvolvimento das atividades relacionadas à gestão da carteira de valores mobiliários e somente na exata medida em que seja necessário o conhecimento de tais Informações Confidenciais.

Fazemos referência ao Manual de Segregação de Atividades e Segurança da Informação do Gestor para mais informações sobre segurança da informação e sobre as regras de sigilo e conduta.

6. Segurança da Informação

As medidas de segurança da informação têm por finalidade a proteção contra ameaças, de modo a garantir a continuidade dos negócios, minimizar riscos e maximizar os retornos aos investidores. Tais medidas, assim como a realização de testes de intrusão anuais e as varreduras de vulnerabilidades, serão implementadas pelos prestadores de serviços de tecnologia da informação – terceirizada para garantia de qualidade e sob responsabilidade da Controladoria, conforme será descrito nos próximos itens deste Manual – com base nas orientações da Diretoria de *Compliance* e Risco, devendo ser observadas por todos os Colaboradores.

Causam situações de risco à Segurança da Informação:

(i) Acessar a sites não relacionados às atividades do Gestor;
(ii) Utilizar mídias ("pen-drives", CDs, entre outras) para armazenamento de arquivos digitais, com exceção das disponibilizadas pelo Gestor;
(iii) Acessar ou salvar informações sensíveis e Informações Confidenciais em pastas virtuais de acesso público;
(iv) Salvar arquivos pessoais na rede de computadores institucional;
(v) Utilizar mídias para transporte de informações não criptografadas;
(vi) Dividir senhas.

As restrições de acesso às Informações Privilegiadas – bem como aos documentos contidos na rede de computadores e sistemas do Gestor - respeitam a divisão de cargos e as linhas pontilhadas do organograma funcional que integra o item 2 deste Manual (Departamento

Técnico/Compliance, Riscos e PLDFT/Controladoria), sendo separados por meio de *Chinese Wall*[2] e de sistemas que permitem a identificação dos detentores de informações, para responsabilização em caso de eventual vazamento.

Exceções às regras supra poderão ser avaliadas pela Diretoria de *Compliance* e Riscos, conforme solicitação formal e devidamente fundamentada e avaliação de conveniência e oportunidade. As evidências da análise das referidas solicitações deverão ser arquivadas em meio eletrônico no Diretório do Gestor, sendo de responsabilidade da Diretoria de *Compliance* e Risco garantir tal procedimento, ainda que por meio da delegação desta atribuição a outro Colaborador.

Mais informações poderão ser encontradas no Anexo II do presente Manual, que contém algumas regras referentes ao Gerenciamento e Segurança de Informações Confidenciais.

7. Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo

De acordo com a Lei nº 9.613, de 03 de março de 1998, bem como a Resolução CVM 50, a prevenção da utilização dos ativos e sistemas do Gestor para fins ilícitos, tais como crimes de lavagem de dinheiro e financiamento ao terrorismo, ocultação de bens, direitos e valores, é dever de todos os Colaboradores.

O Gestor cumpre todas as leis e regulamentos aplicáveis na condução de seus negócios e atividades nas quais está envolvido. Qualquer Colaborador que violar uma lei ou regulamento aplicável à prevenção e combate à lavagem de dinheiro ficará sujeito às sanções disciplinares cabíveis. Caso algum Colaborador viole intencionalmente uma destas leis ou regulamentos, a Diretoria de *Compliance* e Riscos notificará o fato de imediato às autoridades competentes.

Caso o Colaborador suspeite de operações financeiras que possam envolver atividade de corrupção ou lavagem de dinheiro, deverá imediatamente comunicar à Diretoria de *Compliance* e Riscos para que atitudes cabíveis sejam tomadas.

É obrigatório que todos os Colaboradores mantenham arquivada toda e qualquer informação, tais como documentos e extratos que possam vir a ser necessários para o monitoramento ou investigação de possíveis clientes suspeitos de corrupção ou lavagem de dinheiro, desde que nos limites estabelecidos pela Lei 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados).

Para maiores informações, fazemos referência à Política de PLDFT e ao Manual de ID do Gestor, que também incluem disposições referentes às Normas de Combate à Corrupção e às políticas de KYC, KYP e KYE.

8. Treinamentos

Todos os Colaboradores do Gestor receberão cópias do Código de Ética, deste Manual e dos demais normativos internos, devendo analisar as disposições neles contidas e, em caso de dúvidas, acessar a Diretoria de *Compliance* e Riscos para esclarecimentos e orientações.

Adicionalmente, Colaboradores que venham a ser contratados para atuação no Departamento Técnico serão treinados e supervisionados diretamente por um Colaborador Sênior e/ou pela

[2] *Chinese Wall* é o termo utilizado para a referência à barreira de comunicação entre diferentes indivíduos ou setores de uma mesma entidade, visando assegurar (i) o cumprimento das normas que exigem a segregação entre a atividade de administração de carteiras de valores mobiliários e outras atividades relacionadas ou não ao mercado de capitais, (ii) a identificação dos detentores de informações – privilegiadas ou não, conforme abaixo definido -, para eventual responsabilização em caso de vazamento, bem como (iii) a segregação entre ativos financeiros próprios do Gestor e os ativos financeiros de titularidade de terceiros.

Diretoria de Gestão, ficando sob a responsabilidade direta da referida diretoria durante o período de treinamento não inferior a 90 dias.

Haverá ainda incentivo por parte do Gestor para que o Colaborador busque a permanente capacitação técnica e profissional, para tanto disponibilizará subsídios educacionais.

9. Plano de Contingência

O Gestor atua por meio de rotinas elaboradas para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores. Neste sentindo, os seguintes procedimentos são efetuados: "*backup*" mensal de arquivos em "*Hard Disk*" ("HD") externo, "*backup*" semanal e "*backup*" diário em servidores próprios, inclusive de e-mails. Este procedimento evita que o Gestor incorra em prejuízos em caso de contingências, evitando que a qualidade da gestão seja afetada por perda de informações.

Os procedimentos contínuos relacionados à segurança em Tecnologia da Informação ("TI") estão relacionados aos *softwares* de antivírus. Eles protegem durante 24 (vinte e quatro) horas por dia, sem interrupção, a rede interna de computadores do Gestor e o computador de cada Colaborador.

O Gestor tem acesso a atendimento relacionado a TI por diferentes canais, podendo optar pelo atendimento via telefone central, via celular dos Colaboradores e ainda por meio de visitas periódicas e/ou emergenciais.

Dessa forma, por meio da junção dos elementos acima, o Gestor assegura um ambiente de sistema de informação eficiente, confiável e seguro até mesmo em possíveis situações contingenciais.

10. Reporte e Penalidades

A violação deste Manual sujeitará o Colaborador às medidas previstas no Código de Ética do Gestor, sendo dever de todos os Colaboradores informar à Diretoria de *Compliance* e Riscos acerca de violações ou possíveis violações das disposições aqui estabelecidas, de maneira a garantir o tratamento justo e equitativo aos investidores pelo Gestor, zelando, assim, pela sua reputação.

O descumprimento de qualquer regra estabelecida neste Manual implicará, a critério da Diretoria de *Compliance* e Riscos, as seguintes penalidades, a depender da gravidade do descumprimento e da eventual reincidência: (i) advertência por escrito; ou (ii) desligamento.

Qualquer Colaborador que acredite ter violado este Manual ou tenha conhecimento de violação deverá notificar o fato direta e imediatamente à Diretoria de *Compliance* e Riscos, sendo que eventual ação disciplinar levará o reporte em consideração. Ainda, poderão ser tomadas ações disciplinares contra Colaborador que (i) autorize, coordene ou participe de violações a este Manual; (ii) possuindo informação ou suspeita de violações, deixe de reportá-las; (iii) deixe de reportar violações ocorridas que, pelo seu dever de ofício, deveria ter conhecimento ou suspeita; e/ou (iv) promova retaliações, direta ou indiretamente, ou encoraje outros a fazê-lo.

11. Diretor(a) Responsável

Abaixo apresentamos informações cadastrais do Diretor responsável por *Compliance*, Gestão de Riscos e PLDFT do Gestor:

Nome	Alex Alves do Nascimento
Telefone	(21) 3235-0770 ou (11) 3074-0920

Por fim, o Gestor atesta que a Diretoria de *Compliance* e Riscos não está subordinado(a) às demais áreas de atuação, incluindo a gestão de recursos.

12. Atualização

Esta política será submetida à revisão anual ou em períodos inferiores a este, sempre que a Diretoria de *Compliance* e Riscos considerar necessário, com o intuito de preservar as condições de segurança para o Gestor.

ANEXO I – ESCOPO DE ATUAÇÃO DA DIRETORIA DE *COMPLIANCE*, GESTÃO DE RISCO E PLDFT

Temas Normativos

- ✓ Controlar a aderência às novas leis, regulamentações, práticas e diretrizes de autorregulação aplicáveis ao Gestor, e apresentar o resultado de suas verificações periodicamente ao Diretor de Gestão;
- ✓ Controlar e monitorar as licenças legais, registros e certificações necessárias (registros na CVM, ANBIMA e demais aplicáveis), bem como sua renovação/manutenção junto às autoridades;
- ✓ Auxiliar a alta administração do Gestor no relacionamento com órgãos reguladores e assegurar que as informações requeridas sejam fornecidas no prazo e qualidade requeridos;
- ✓ Realizar revisões e relatórios obrigatórios nas frequências definidas na legislação em vigor.

Boas Práticas

- ✓ Designar pessoa responsável pela promoção e acessibilidade das informações necessárias para o cumprimento das normas internas legais, infralegais e de autorregulação, bem como pela coleta dos termos de ciência e aderência assinados por todos os Colaboradores;
- ✓ Estabelecer controles para que todos os Colaboradores do Gestor atuem com independência e atentem ao devido dever fiduciário para com seus clientes, evitando conflitos de interesse;
- ✓ Garantir que os controles internos sejam compatíveis com os riscos do Gestor em suas atividades, 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;
- ✓ Analisar informações, indícios ou identificar, administrar eventuais conflitos de interesses ou descumprimentos regulatórios e de políticas e normas; e
- ✓ Comunicar aos órgãos competentes, nos prazos regulatórios, a respeito de eventuais descumprimentos normativos.

Governança

- ✓ Aprovar novos procedimentos e submeter novas políticas e manuais à aprovação dos sócios do Gestor;
- ✓ Apresentar o resultado de seus controles e verificações à Diretoria ou em Reunião de Sócios;
- ✓ Monitorar e buscar a efetiva aplicação dos documentos de *Compliance* e Controles Internos;
- ✓ servir como canal para comunicações de desconformidades regulatórias e/ou de temas relacionados ao Código de Ética do Gestor; e

ANEXO II – SISTEMA DE GERENCIAMENTO E SEGURANÇA DE INFORMAÇÕES

O Gestor considera o gerenciamento das informações um assunto de âmbito estratégico, uma vez que as decisões que permeiam a gestão de seus ativos dependem da confiabilidade, segurança e acessibilidade ao sistema de gerenciamento de informações.

Para atingir estes objetivos, o Gestor estabeleceu regras de *Compliance* e de gestão de segurança em TI.

Gerenciamento de Informações Confidenciais

Quanto aos parâmetros de C*ompliance*, o Gestor define os perfis de acesso de cada usuário da rede interna de computadores de forma que as Informações Confidenciais fiquem acessíveis somente por determinadas pessoas do Gestor, autorizadas pela Diretoria de *Compliance* e Riscos. Ficam preservadas as informações de clientes e ao mesmo tempo evitam-se problemas relacionados a conflitos de interesses ou uso indevido de Informações Confidenciais.

Além disso, o controle de tráfego de dados entre Colaboradores é realizado por meio de sistemas de "*firewall*" e controle de acessos à rede de computadores, que são responsáveis pela proteção de Informações Confidenciais e pela segregação das informações entre os grupos de Colaboradores que a elas devem ter acesso. Tais controles são estabelecidos nas autorizações de perfis de acesso e restrição de usuários da rede. Dessa forma, controla-se quem efetivamente acessou determinados dados e/ou sistemas e ficam impedidos acessos não autorizados.

Assim, foram definidos níveis de acesso para os membros do Gestor.

No que se refere ao gerenciamento de riscos referentes à segurança da informação, o Gestor atuará por meio de rotinas elaboradas por prestadores de serviço especializados para assegurar um ambiente resguardado de qualquer tipo de risco para as informações e para a rede interna de computadores, evitando que a qualidade da gestão seja afetada por contingências.

Estrutura de Tecnologia de Informação e Hardware:

Em complemento às informações contidas no item acima, o Gestor terá uma rede integrada de computadores, revisados quanto à capacidade, segurança e nível de atualização de seus componentes, com o suporte técnico de empresa terceirizada contratada. Ainda, serão realizados "*backup*" mensal de arquivos em "*Hard Disk*" ("HD") e *backups* em servidores, inclusive de e-mails. Além disso, serão adotados procedimentos contínuos relacionados aos *softwares* de antivírus, responsáveis por proteger, durante 24 (vinte e quatro) horas por dia, sem interrupção, a rede interna de computadores do Gestor e o computador de cada colaborador.

Ainda, com relação aos e-mails, o Gestor utilizará equipamentos atualizados e seu servidor de e-mails será hospedado junto a Microsoft, através do *Exchange Online (Office 365 Business Standard)*, o que garantirá alta disponibilidade e segurança e viabilizará o trabalho remoto e via computadores reserva, se e quando necessário, sem prejuízo da manutenção de registros que irá viabilizar a realização de auditorias e inspeções nos termos dos manuais e políticas da gestora.

No que tange aos *IDs* dos Colaboradores e aos computadores, sua administração ocorrerá de forma centralizada através de servidor, onde (i) usuários e suas atividades podem ser monitorados; (ii) o particionamento das pastas é viabilizado; e (iii) os perfis de acesso são configurados conforme as prerrogativas e necessidades inerentes aos cargos dos colaboradores.

Adicionalmente, com relação à estrutura de telefonia, o Gestor terá PABX com canais na sala de gestão e linhas móveis corporativas (para uso dos colaboradores sempre que necessário) como meios de comunicação.

Por fim, todos os Colaboradores do Gestor terão acesso a atendimento relacionado aos sistemas de tecnologia da informação por diferentes canais, podendo optar pelo atendimento via telefone central, via celular dos colaboradores e, ainda, por meio de visitas periódicas e/ou emergenciais.