MTR
asset

MANUAL DE SEGREGAÇÃO DE ATIVIDADES E SEGURANÇA DA INFORMAÇÃO

MTR ASSET GESTORA DE RECURSOS LTDA.

Versão 2.0
Março/2026

[A MTR Asset Gestora de Recursos Ltda. encontra-se em processo de habilitação junto ao convênio ANBIMA/CVM na categoria Administrador de Carteiras de Valores Mobiliários.]

MTR
asset

SUMÁRIO

1. OBJETIVO E ABRANGÊNCIA 3
2. ESTRUTURA 3
3. SEGREGAÇÃO FÍSICA 4
4. SEGREGAÇÃO FUNCIONAL 4
5. *CHINESE WALL* E INFORMAÇÕES PRIVILEGIADAS – SIGILO E CONDUTA 5
6. CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA 6
7. REPORTE, PENALIDADES E RESPONSABILIDADE 9
8. ACOMPANHAMENTO 9
9. RESPONSÁVEIS 9
10. VIGÊNCIA E ATUALIZAÇÃO 10

ANEXO I - SISTEMA DE GERENCIAMENTO E SEGURANÇA DE INFORMAÇÕES 11

MTR
asset

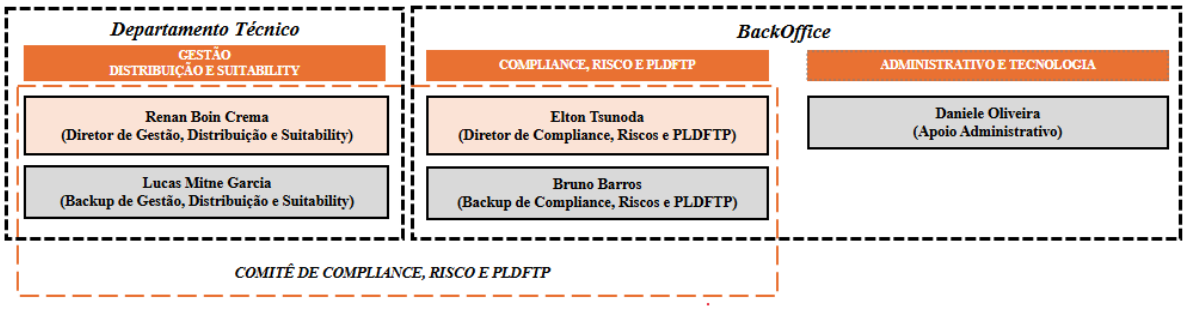
1. OBJETIVO E ABRANGÊNCIA

1.1. Este Manual de Segregação de Atividades e Segurança da Informação ("Manual") da MTR Asset Gestora de Recursos Ltda. ("MTR Asset") foi elaborado de acordo com os artigos 27 e 28 da Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM 21") e tem como finalidade: **(i)** garantir a segregação física de instalações entre a área de Gestão e de Distribuição e Suitability ("Departamento Técnico") e a área de *Compliance* e Risco responsável também por PLDFTP; **(ii)** assegurar o bom uso de instalações, equipamentos e informações comuns; **(iii)** preservar Informações Confidenciais, conforme definição estabelecida abaixo, e permitir a identificação das pessoas que tenham acesso a elas; e **(iv)** restringir o acesso a arquivos e permitir a identificação das pessoas que tenham acesso a informações confidenciais.

1.2. Este Manual é aplicável a todos os sócios, diretores, funcionários e estagiários que participem, de forma direta, das atividades diárias e negócios da MTR Asset ("Colaboradores" e, no singular, "Colaborador").

1.3. Adicionalmente, o Manual também abrangerá as questões relacionadas à Segurança da Informação, sob liderança da área de *Compliance*, Risco e PLDFTP. A área poderá, a qualquer tempo, e se assim avaliado como conveniente, contratar demais prestadores de serviços qualificados, visando garantir a eficiência e segurança compatíveis com as necessidades da MTR Asset, de seus Colaboradores, investidores, bem como a responsabilização dos envolvidos em caso de violação (e/ou vazamentos) de dados.

2. ESTRUTURA



2.1. Considerando a estrutura da MTR Asset, refletida no Manual de Regras, Procedimentos e Descrição de Controles Internos ("Manual de Compliance") e no organograma acima, foram desenvolvidas regras aplicáveis à **(i)** segregação física entre as áreas do Departamento Técnico e a área de *Compliance*, Risco e PLDFTP; **(ii)** segregação funcional dos profissionais; **(iii)** *Chinese Wall*; e **(iv)** Segurança da Informação.

2.2. No que se refere a ao item (iv) acima, a área de *Compliance*, Risco e PLDFTP, é responsável pela área de Tecnologia e Segurança da Informação, e em conjunto

com os prestadores de serviço de tecnologia da informação eventualmente contratados, será responsável pela implantação e racionalização de processos, manutenção dos sistemas de informática, segurança da informação com controle de acesso dos usuários e *backup* de dados.

3. SEGREGAÇÃO FÍSICA

3.1. O espaço físico que será utilizado pelas áreas de Gestão e de Distribuição e *Suitability* será segregado do espaço físico destinado à área de *Compliance*, Risco e PLDFTP.

3.2. O espaço reservado à área de *Compliance*, Risco e PLDFTP será, por sua vez, limitado aos Colaboradores envolvidos nas referidas atividades, sendo o controle de acesso realizado por meio de fechaduras acionadas com cartão de aproximação.

3.3. Cabe destacar que a segregação física de instalações entre o Departamento Técnico e a área de Distribuição e *Suitability* não é necessária, nos termos do Art. 27, § único da Resolução CVM 21.

3.4. Cada Colaborador possui equipamento próprio com login e senha, e os seus acessos estão vinculados ao cargo desempenhado. Desta forma, Colaboradores não tem acesso às informações de outras áreas, em especial, a área responsável pela atividade de administração de carteiras de valores mobiliários.

3.5. O uso de instalações em áreas não segregadas deverá respeitar as regras de boa convivência, respeito, cuidado e diligência que todo Colaborador nas suas instalações, equipamentos e informações particulares.

3.6. Os Colaboradores desligados deverão ter seu cartão de aproximação e acesso revogado no momento do desligamento.

4. SEGREGAÇÃO FUNCIONAL

4.1. A segregação funcional entre as áreas de (i) Gestão e Distribuição; (ii) Compliance, Riscos e PLDFTP; e (iii) Administração da MTR Asset, observará a estrutura organizacional definida no Manual de Compliance e no organograma funcional da instituição, de forma a assegurar a independência técnica e a ausência de interferência indevida especialmente entre atividade de gestão de recursos das demais atividades exercidas pela pessoa jurídica.

4.2. A área de Gestão e Distribuição é de responsabilidade do Diretor de Gestão, que acumula as funções relativas às atividades de distribuição e suitability, cabendo-lhe, com apoio exclusivo de seu analista (*backup*), a condução das análises de investimento, a definição de estratégias, a tomada de decisões de compra e venda de ativos e a execução e retransmissão de ordens, bem como o relacionamento comercial e a adequação de produtos ao perfil dos investidores.

4.3. A área de Compliance, Riscos e PLDFTP, controlada pelo Diretor de Compliance, Riscos e PLDFTP, é responsável pela supervisão do cumprimento regulatório, pela gestão e monitoramento dos riscos, pela implementação das políticas de prevenção à lavagem de dinheiro, pelo acompanhamento dos controles internos e pela segurança da informação. O analista alocado nessa área atua exclusivamente em atividades de monitoramento, revisão, reporte, testes de controles, sem participação na originação de negócios, na definição de estratégias de investimento ou na execução de ordens, nem vínculo com metas comerciais ou de performance dos fundos.

4.4. A área Administrativa será responsável pelas atividades administrativas relacionadas à estrutura física, tecnológica e operacional da MTR Asset, incluindo a gestão das instalações, dos recursos de tecnologia da informação e dos processos de suporte à operação. Caberá a essa área supervisionar os prestadores de serviços tecnológicos, contábeis, jurídicos e demais fornecedores contratados em base ad hoc, bem como, quando necessário, contratar prestadores especializados para manutenção de sistemas, controle de acessos, rotinas de backup e medidas de segurança da informação, de forma a assegurar a continuidade, integridade e regularidade das operações da MTR Asset.

4.5. O processo de avaliação e gerenciamento de riscos permeia todas as etapas do processo decisório de investimento, de modo que o monitoramento, incluindo a elaboração de relatórios e a verificação de limites, é exercido sob responsabilidade conjunta da área de Gestão e da área de Compliance e Riscos, responsável também por PLDFTP, em consonância com a Política de Gestão de Riscos da MTR Asset.

4.6. Atualmente os Colaboradores da MTR Asset, com exceção dos sócios-investidores, não exercem qualquer função ou cargo equivalente em outras sociedades, de forma a preservar a independência de sua atuação profissional e evitar potenciais conflitos de interesses.

4.7. Adicionalmente, as atividades das sociedades nas quais os Diretores da MTR Asset figuram como sócios ou administradores e que pudessem, em tese, se sobrepor ou conflitar com a sua atividade exercida na MTR Asset tiveram suas operações encerradas quando do credenciamento da MTR Asset como administradora de carteiras de valores mobiliários, mantendo-se ativas apenas para fins de recebimento de pagamentos de serviços prestados no passado.

5. *CHINESE WALL* E INFORMAÇÕES PRIVILEGIADAS – SIGILO E CONDUTA

5.1. Para fins deste e dos demais normativos internos da MTR Asset, informações privilegiadas são aquelas consideradas relevantes para a tomada de decisões de investimento e/ou desinvestimento, que não tenham sido divulgadas publicamente, e que sejam obtidas em decorrência do cargo ocupado pelos Colaboradores da MTR Asset (por exemplo, de relação profissional ou pessoal

mantida com um cliente ou com pessoas vinculadas a investidas dos fundos de investimento geridos) ("Informações Privilegiadas").

5.2. As Informações Privilegiadas devem ser mantidas em sigilo pelos Colaboradores que a elas tiverem acesso, visando evitar práticas de *Insider Trading* e *Tipping*, conforme descrito nos capítulos seguintes deste Manual.

5.3. As restrições de acesso às Informações Privilegiadas – bem como aos documentos contidos na rede de computadores e sistemas da MTR Asset – respeitam a divisão de cargos do organograma funcional que integra o item 2 deste Manual e serão implementadas por meio de controles (as Diretrizes de Segurança da Informação, conforme descritos no item 5 abaixo) que, em conjunto, formam o *Chinese Wall* da MTR Asset.

5.4. *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 da MTR Asset e os ativos financeiros de titularidade de terceiros.

5.5. Exceções às regras supra, no entanto, poderão ser avaliadas pela área de *Compliance*, Riscos e PLDFTP, 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 da MTR Asset, sendo de responsabilidade da área de *Compliance*, Riscos e PLDFTP garantir tal procedimento, ainda que por meio da delegação desta atribuição a outro Colaborador.

6. CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

6.1. Além das disposições abaixo, os Colaboradores deverão atender ao disposto no Manual de Compliance e na Política de Prevenção à Lavagem de Dinheiro, Financiamento ao Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa ("Política de PLDFTP").

6.2. As disposições acerca de Confidencialidade, Segurança da Informação e Cibersegurança serão implementadas pela área de *Compliance*, Risco e PLDFTP.

Informações Confidenciais:

6.3. No exercício de suas atividades, os Colaboradores poderão ter acesso a informações de clientes da MTR Asset, bem como de terceiros, que não sejam de conhecimento do público em geral e que, portanto, possam ser consideradas

confidenciais. Assim, as Informações Pessoais[1], as Informações da MTR Asset[2], as Informações Sigilosas[3], as Informações Privilegiadas e toda e qualquer informação a que clientes, Colaboradores, prestadores de serviços, conforme aplicável, e parceiros tenham acesso, a respeito de, mas não se limitando, a produtos, projetos, processos, tecnologias, procedimentos e planejamentos, independentemente da forma de acesso (estruturada ou desestruturada, impressa, arquivada em mídia eletrônica, verbal) e de ter ou não sido direcionada ao receptor serão consideradas como confidenciais ("Informações Confidenciais" ou, no singular, "Informação Confidencial").

6.4. Adicionalmente, cumpre à MTR Asset esclarecer que 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.

6.5. A MTR Asset e os 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 área de Compliance, Risco e PLDFTP, responsável pela área de Tecnologia e Segurança da Informação, para que decida, em conjunto com os demais membros da Diretoria da MTR Asset, quanto à sua regularidade e necessidade.

6.6. O Colaborador que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais pode ser repassada para terceiros sem o consentimento prévio e por escrito do departamento jurídico. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pela MTR Asset.

6.7. Excetuam-se da obrigação de manutenção de confidencialidade disposta nesta Política: (i) o atendimento a quaisquer determinações decorrentes de lei ou emanadas do Poder Judiciário ou Legislativo, tribunal arbitrais e de órgãos públicos administrativos, desde que analisado e autorizado previamente e por escrito pelo departamento jurídico; (ii) a divulgação das informações confidenciais aos representantes (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros) e empregados das partes; e (iii) as informações confidenciais que forem divulgadas após o consentimento, por escrito, do departamento jurídico.

---

[1]Qualquer informação que identifique ou possa identificar uma pessoa física específica com o uso de recursos razoáveis.
[2]Qualquer informação produzida por Colaboradores e prestadores de serviços, conforme aplicável, toda informação gerada pela atividade intelectual relacionada as funções da MTR Asset, expressas em papel ou em meios digitais, armazenados em qualquer tipo de mídia.
[3]Parcela das Informações Confidenciais, conforme abaixo definido, que, caso venham à tona, podem resultar em perda do nível de segurança da MTR Asset.

Diretrizes de Segurança da Informação e Cibersegurança:

6.8. As Diretrizes de Segurança da Informação correspondem aos controles estabelecidos pela MTR Asset, conforme orientação da área de *Compliance*, Riscos e PLDFTP, e 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 estão sob a responsabilidade da área de Compliance, Risco e PLDFTP e devem ser observadas por todos os Colaboradores.

6.9. 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. Causam situações de risco à Segurança da Informação:

(i) Acessar a sites não relacionados às atividades da MTR Asset;
(ii) Utilizar mídias ("pen-drives", CDs, entre outras) para armazenamento de arquivos digitais, com exceção das disponibilizadas pela MTR Asset;
(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; e
(vi) Dividir senhas.

6.10. Apenas os equipamentos e software disponibilizados e/ou homologados pela área de Tecnologia da Informação da MTR Asset podem ser instalados e conectados à rede da empresa, salvos exceções aprovadas pela área de Tecnologia da Informação e/ou Diretoria de *Compliance*, Riscos e PLDFTP.

6.11. A MTR Asset disponibiliza rede Wi-Fi com acesso internet para visitantes.

6.12. Todos os ativos de informação devem ser devidamente guardados ou destruídos, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização.

Uso da Internet

6.13. O uso da internet pelos Colaboradores é permitido e encorajado desde que seu uso seja aderente aos objetos e atividade fins do negócio da MTR Asset. Entretanto, é estritamente proibido:

(i) Usar o computador para executar quaisquer tipos ou formas de fraudes, ou software pirata;
(ii) Usar a internet para envio de material ofensivo ou de assédio para outros usuários;
(iii) Baixar (download) software comercial ou qualquer outro material cujo direito pertença a terceiro (copyright), sem ter um contrato de licenciamento ou outros tipos de licenciamento;
(iv) Atacar e/ou pesquisar em áreas não autorizadas (hacking);

(v) Criar ou transmitir material difamatório; e
(vi) Executar atividade que desperdice os esforços do pessoal técnico ou dos recursos de rede.

7. REPORTE, PENALIDADES E RESPONSABILIDADE

7.1. É dever de todo Colaborador informar à área de *Compliance,* Risco e PLDFTP e sobre violações ou possíveis violações das disposições referentes à Segregação de Atividades e à Segurança da Informação, respectivamente, contidas neste Manual, sendo certo que o descumprimento de qualquer regra neles estabelecida implicará, a critério do Comitê de *Compliance*, Risco e PLDFTP, na aplicação de uma ou mais das seguintes penalidades, a depender da gravidade do descumprimento e de eventual reincidência: (i) advertência por escrito; ou (ii) desligamento.

7.2. Qualquer Colaborador que acredite ter violado este Manual, ou tenha conhecimento de violação, deverá notificar o fato direta e imediatamente à área de *Compliance*, Risco e PLDFTP, conforme aplicável nos termos do parágrafo acima, sendo que eventual ação disciplinar levará o reporte em consideração.

7.3. 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.

8. ACOMPANHAMENTO

8.1. Caso haja ocorrência, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas neste Manual, caberá ao Diretor de *Compliance*, Risco e PLDFTP, disponibilizar ao Comitê de *Compliance*, Risco e PLDFTP os registros eletrônicos disponíveis para apuração da conduta dos Colaboradores.

8.2. A Diretoria de *Compliance*, Risco e PLDFTP terão acesso a todo conteúdo que está na rede de computadores da MTR Asset e poderão acessar tal conteúdo caso haja necessidade. A confidencialidade das informações será respeitada e seu conteúdo será disponibilizado somente para fins legais, garantindo, assim, verificação dos responsáveis por eventuais vazamentos e outras formas de violação.

9. RESPONSÁVEIS

9.1. Abaixo apresentamos informações cadastrais do Diretor de *Compliance* e Risco, responsável também por PLDFTP, responsável pela implementação das regras relativas à Confidencialidade e Segurança da Informação, da MTR Asset:

Diretor de *Compliance* e Risco	Elton Tsunoda
E-mail	elton.tsunoda@mtrasset.com.br
Telefone	(11) 5589-3000

9.2. Por fim, a MTR Asset atesta que a Diretoria de *Compliance*, Risco e PLDFTP não está subordinada às demais áreas de atuação, incluindo a gestão de recursos e distribuição.

10. VIGÊNCIA E ATUALIZAÇÃO

10.1. Este Manual será revisado anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterado a qualquer tempo em razão de circunstâncias que demandem tal providência.

Versão	Data	Responsabilidade
2	18/03/2026	Elton Tsunoda

MTR
asset

ANEXO I - SISTEMA DE GERENCIAMENTO E SEGURANÇA DE INFORMAÇÕES

A MTR Asset 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, a MTR Asset estabeleceu as seguintes regras:

Gerenciamento de Informações Confidenciais

Quanto aos parâmetros, a MTR Asset 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 da MTR Asset, autorizadas conforme as linhas pontilhadas contidas no organograma funcional do item 2 deste Manual. 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 Comitê de *Compliance*, Risco e PLDFTP, e para as áreas de Gestão e *Compliance*, Risco e PLDFTP.

No que se refere ao gerenciamento de riscos referentes à segurança da informação, a MTR Asset atuará por meio de rotinas elaboradas pela área de *Compliance*, Risco e PLDFTP, 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, a MTR Asset 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*" diários de arquivos inclusive de e-mails em serviço em de nuvem (Nuvem Microsoft) contratado para tal finalidade. 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 da MTR Asset e o computador de cada Colaborador.

Ainda, com relação aos e-mails, a MTR Asset utilizará equipamentos atualizados e seu servidor de e-mails será hospedado junto a Microsoft, através 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 irá viabilizar a realização de auditorias e inspeções nos termos dos manuais e políticas da MTR Asset.

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 poderão 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, a MTR Asset terá à disposição o Microsoft Teams com canais na sala de gestão e com usuários exclusivos (para uso dos Colaboradores sempre que necessário) como meios de comunicação, além de dispor de uma linha de telefone fixa, para ligações externas.

Por fim, todos os Colaboradores da MTR Asset 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.