PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS NEGÓCIOS
(“Plano”)

JULHO/2026

LESTE

ÍNDICE

1. Apresentação do Grupo Leste

O presente Plano é aplicável à Leste Financial Services Gestão de Recursos Ltda. ("LFS"), à Leste Credit Gestão de Recursos Ltda. ("LCBR") e à Leste Administração de Recursos Ltda. ("LAR", e, em conjunto com a LFS e a LCBR, "Gestoras").

2. Objetivo

Este Plano tem como objetivo definir os procedimentos a serem adotados pelos sócios, administradores, funcionários e por todos aqueles que, de alguma forma, auxiliem no desenvolvimento das atividades das Gestoras ("Colaboradores"), em decorrência da ocorrência de eventuais contingências, de modo a evitar a descontinuidade operacional por problemas que impactem o funcionamento das Gestoras no âmbito de sua atividade de gestão de recursos. Foram estipuladas estratégias e planos de ação com o intuito de garantir que os serviços essenciais das Gestoras sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou desastre.

3. Base Legal

(i) Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21");
(ii) Resolução CVM nº 50, de 31 de agosto de 2021, conforme alterada ("Resolução CVM nº 50");
(iii) Resolução CVM nº 175, de 23 de dezembro de 2022, conforme alterada ("Resolução CVM nº 175"), e seus Anexos Normativos;
(iv) Ofício-Circular/CVM/SIN/Nº 05/2014;
(v) Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("Anbima") de Ética ("Código ANBIMA de Ética");
(vi) Código de Administração e Gestão de Recursos de Terceiros da Anbima ("Código de AGRT");
(vii) Regras e Procedimentos de Administração e Gestão de Recursos de Terceiros, especialmente seu Anexo Complementar III;
(viii) Lei nº 12.846, de 1º de agosto de 2013, e Decreto nº 11.129, de 11 de julho de 2022, conforme alterados ("Normas de Anticorrupção");
(ix) Lei nº 9.613, de 03 de março de 1998, conforme alterada; e
(x) Demais manifestações e ofícios orientadores dos órgãos reguladores e autorreguladores aplicáveis às atividades das Gestoras.

2.1. Interpretação e Aplicação do Plano de Contingência

Para fins de interpretação dos dispositivos previstos neste Plano, exceto se expressamente disposto de forma contrária: (a) os termos utilizados neste Plano terão o significado atribuído na Base Legal acima; (b) as referências a Fundos abrangem as Classes e Subclasses, se houver; e (c) as referências a Regulamento abrangem os anexos e apêndices, quando aplicável, observado o disposto na Base Legal acima.

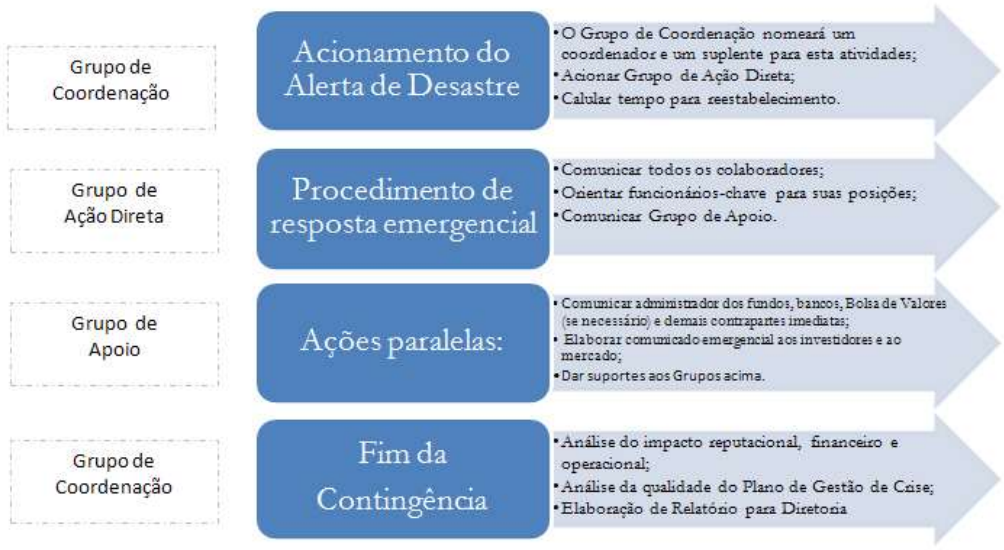
4. Equipe de Contingência

Para coordenar todas as ações necessárias no âmbito deste Plano, bem como promover o treinamento adequado e as ações para restabelecimento da situação de atividade normal das Gestoras, foram definidos os seguintes responsáveis pela Equipe de Contingência: **(1)** o Head da equipe de Tecnologia da Informação (Coordenador de Contingência); **(2)** a Diretora de *Compliance* (em caso de ausência do Coordenador de Contingência, esta se tornará a responsável pelo Plano e pela Ação Direta); e **(3)** os Analistas da equipe de Tecnologia da Informação, que atuarão no apoio das atividades relacionadas.

Essas pessoas deverão tomar as decisões necessárias para acionar este Plano, se e quando necessário, tomando tal decisão em conjunto ou, no caso de impossibilidade, com os demais administradores das Gestoras.

Posição	Atribuição
Coordenação	• Nomear os participantes do plano; • Revisar periodicamente a documentação atualizada dos sistemas; • Testar a integridade das cópias redundantes das informações e dados da organização; • Disponibilizar recursos para ação de resposta e calcular tempo de recuperação; • Acionar o grupo de atuação direta, quando necessário; • Promover treinamento dos colaboradores; • Promover exercícios simulados; • Garantir a revisão periódica do plano; • Enviar relatório final de situação para Diretoria; • Elaborar relatório final de situação.
Ação Direta	• Planejamento das ações de resposta relacionadas à sua área (sistêmica, operacional, posições-chave e comunicação ao mercado); • Determinar as orientações para as equipes de atuação; • Seguir os procedimentos descritos para o cenário; • Auxiliar, no que for necessário, nas ações de combate; • Avaliar a participação do grupo após um incidente.
Apoio	• Seguir as orientações do grupo de coordenação e de ação direta; • Executar as atividades de provimento de recursos.

4.1. Fluxograma de acionamento do Plano



5. Metodologia

O Plano é dividido em 2 (dois) segmentos:

(i) Plano de Continuidade Operacional – relata os sistemas implantados nas diversas áreas para garantir o acesso ininterrupto e íntegro às informações constantes de nossas bases e servidores; e
(ii) Plano de Gestão de Crise e Recuperação de Desastre – cujo propósito é definir as responsabilidades de cada membro das equipes envolvidas, no caso de acionamento de contingência – antes, durante e depois da ocorrência do incidente. Este plano também dispõe sobre os procedimentos a serem executados pela equipe até a volta da normalidade.

5.1. Plano de Continuidade Operacional

O Plano de Continuidade Operacional se sustenta em arquitetura de serviços e dados hospedados em uma nuvem privada e contingenciada em tempo real com o data center localizado na matriz do Grupo Leste.

As informações armazenadas na nuvem privada do Grupo Leste possuem um procedimento de cópia (*backup*) em camadas, GFS, contemplando retenções diárias, mensais, semestrais, anuais e de longo prazo, inclusive por período de até 5 anos, de acordo com a criticidade dos dados, requisitos legais, regulatórios e operacionais

aplicáveis. A área de Tecnologia realiza testes periódicos de restauração, de modo a avaliar a efetividade dos backups e a capacidade de recuperação dos dados e sistemas em caso de falha, indisponibilidade, exclusão indevida, incidente cibernético ou desastre.

Os backups deverão ser protegidos contra acesso indevido, perda, alteração não autorizada, exclusão acidental ou exclusão maliciosa. Sempre que tecnicamente viável, deverão ser adotados mecanismos de retenção, criptografia, cópias segregadas, armazenamento seguro e proteção contra ransomware.

Com o objetivo de restabelecer o ambiente operacional no menor tempo possível, os dados são replicados. Isso é feito através do DFS para arquivos de dados e da Replicação SQL para a réplica das bases de dados corporativas. Isso garante que, em caso de indisponibilidade prolongada do ambiente privado na nuvem, os usuários possam retomar suas atividades utilizando uma infraestrutura local. Essa estratégia é implementada para minimizar o tempo de inatividade e garantir a continuidade dos negócios.

Em caso de indisponibilidade de um dos nossos escritórios, as Gestoras podem realizar o acesso remoto, via VPN (Client2Site), para um dos nossos escritórios localizados no RJ, SP ou Miami, ou diretamente para a nuvem.

O tempo de replicação dos dados é dado pela taxa de transmissão de dados entre os escritórios e a nuvem privada. Todos os escritórios e a nuvem privada estão interligados através de uma rede criptografada por meio de VPN, e são contingenciados por duas operadoras de internet com alta taxa de transmissão e recebimento de dados com padrão de qualidade empresarial. A replicação dos dados pode ocorrer em menos de um segundo ou até poucos minutos em função da distância física a ser percorrida e do volume de dados alterados, entre outros fatores. A taxa média de transmissão de dados ocorre com uma média de 25ms, com monitoramento ativo de ferramentas especializadas.

Para assegurar o bom funcionamento deste mecanismo o Grupo Leste conta ainda com:

(i) Duplicidade de equipamentos para processamento, core de rede e *firewall*;
(ii) Redundância para fontes e discos nos servidores, inclusive com troca de discos sem paradas;
(iii) Fornecimento de energia por nobreak (local ou predial) para estações de trading, servidores e ativos de rede somados a facilidade de um gerador de energia da edificação;
(iv) Todos os servidores em cada site são virtualizados com um pool compartilhado de recursos em duas máquinas distintas;

(v) Suporte 24x7 com atendimento em até 4h dos fabricantes dos equipamentos para reparos nos equipamentos principais e spares pré-configurados para os demais;

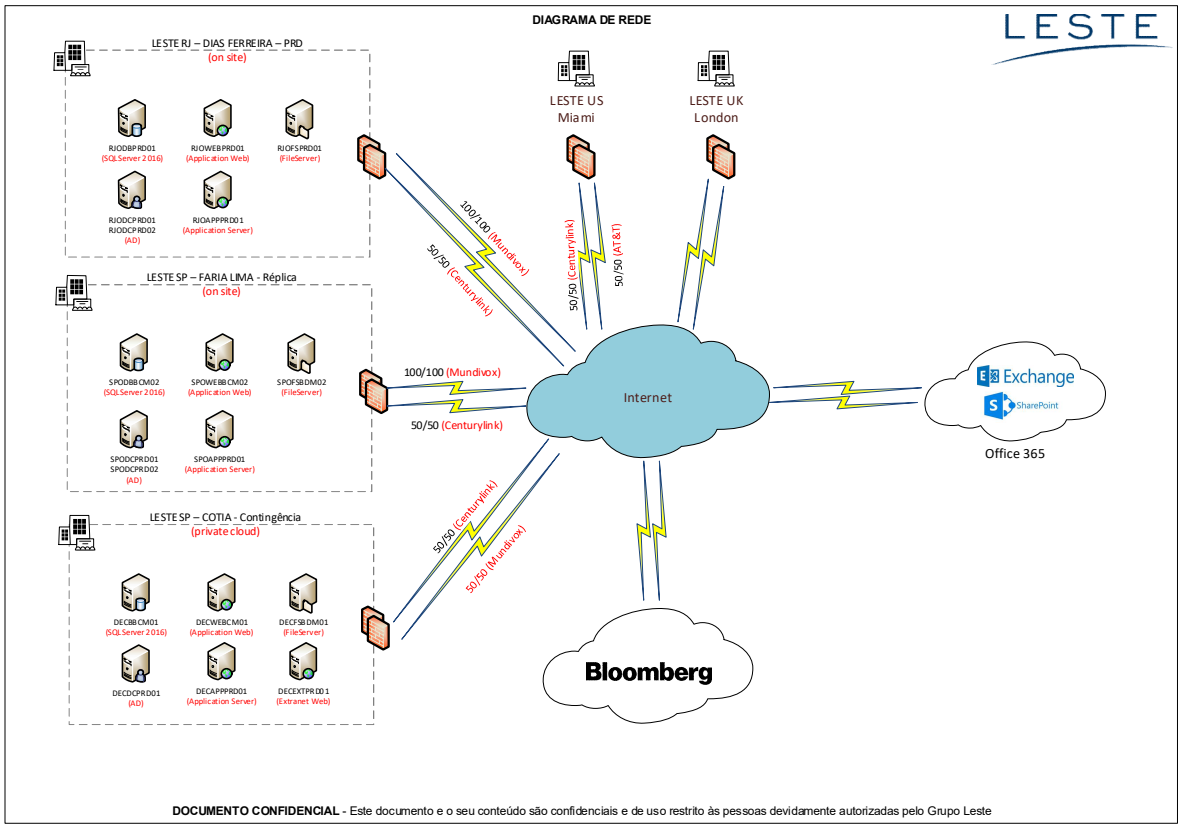
(vi) Suporte 24x7 com SLA de até 4h para restabelecimento dos serviços de Cloud, com monitoramento ativo dos nossos servidores;

(vii) Suporte 24x7 com SLA de até 2h para restabelecimento dos links de internet, com monitoramento ativo e contingenciamento pelos nossos diferentes escritórios;

(viii) Monitoramento ativo do tráfego de rede e internet, segregado em diferentes VLANs para voz e dados.

Ainda, cumpre destacar que são executados semestralmente testes e auditorias de rede, assim como a validação do ambiente de *disaster recovery*. Os ativos são monitorados pelos sistemas Zabbix e Grafana, com antecipação de problemas e notificação em tempo real. Qualquer evento suspeito pode ser monitorado pelos logs do *firewall*, além do serviço de notificação da equipe técnica por e-mail.

5.2. Mapa de Rede – Contingência Remota



5.2.1. Estrutura de TI e *NoBreaks*

O escritório do Rio de Janeiro possui um Data Center contendo 3 racks de servidores e 1 rack de dados, com controle de acesso por senha, sistema de NoBreak redundante de 80 KVA e autonomia estimada de 1 hora, além de gerador predial com autonomia de 8 horas sem abastecimento (explicado em detalhes abaixo), quatro servidores Dell PE R720, 64 GB de RAM (até 768 GB), 3 TB SAS em RAID 5 e 2 processadores E5-2630v2. O Data Center ainda possui sistema de monitoramento de ambiente, com sensores de temperatura, umidade, fumaça e câmera, assim como sistema de controle de incêndio separado, além de sistema redundante de ar-condicionado. A rede conta com switches Dell, firewalls Fortigate com spare e NAS Dell R530 com 18 TB para backup local. A telefonia utiliza central Avaya IP Office, com 2 canais E1, licença para gravações de ligações e ramais Avaya IP 9641 com licença mobile. O sistema de vigilância é Intelbras, com câmeras Full HD.

O escritório de São Paulo possui sala contendo dois racks, com chave e controle de acesso, quatro *nobreaks* EATON, sendo 2 de 3 KVA e 2 de 1,5 KVA, dois servidores Dell PE R720, 64 GB de RAM (até 768 GB), 3 TB SAS em RAID 5, com 2 e 1 processadores E5-2630v2, respectivamente. O CPD ainda possui sistema de monitoramento de ambiente APC Netbotz, com sensores de temperatura, umidade, fumaça e câmera, assim como sistema de controle de incêndio separado. A rede conta com *switches* Dell e HP, *firewalls Fortigate* com *spare* e NAS Dell R530 com 14 TB para backup local. A telefonia utiliza central Avaya IP Office, com 1 canal E1, licença para gravações de ligações e ramais Avaya IP 9641 com licença mobile. O sistema de vigilância é Tecvoz IP, com câmeras Panasonic IP.

O escritório de Miami possui sala contendo um rack, com chave e controle de acesso, dois *nobreaks* EATON, sendo 2 de 3 KVA e 2 de 1,5 KVA, um servidor Dell PE R720, 64 GB de RAM (até 768 GB), 3 TB SAS em RAID 5 e 1 processador E5-2630v2. A rede conta com switches Dell e firewalls Fortigate com spare. A telefonia utiliza central Avaya IP Office, com 1 canal E1, licença para gravações de ligações e ramais Avaya IP 9641 com licença mobile.

Na nuvem privada, Tier III, há um ambiente com 64 cores de processamento, 512 GB de RAM e 10 TB de disco em RAID 5, atrás de firewall por hardware, com link de internet de 100 Mbps dedicado e interligado aos escritórios do Grupo Leste por meio de VPNs criptografadas.

Segue o escalonamento de contingência elétrica do condomínio Leblon Corporate – Sede Rio de Janeiro.

(i) Alimentação principal do condomínio pela concessionária;
(ii) Ao cair a alimentação da concessionária, instantaneamente os *nobreaks* 01 e 02 assumem as cargas do Data Center;

(iii) O gerador parte no mesmo instante em que falta a alimentação da concessionária, porém só assume toda a carga do prédio 40 segundos após sua partida. Nesse período, as cargas essenciais ficam somente pelo nobreak (8 horas de autonomia, aproximadamente);
(iv) Todo o prédio, incluindo tomadas comuns, ar-condicionado e todos os elevadores, ficam alimentados pelo gerador;
(v) A empresa de manutenção predial, *Markbuilding*, possui contrato com uma mantenedora de geradores, que, após a abertura do chamado, deve abastecer os geradores em até 4 horas; e
(vi) Com o retorno da energia da concessionária, o gerador só deixa de funcionar após 1 minuto. Esse intervalo é necessário para evitar que eventuais oscilações na energia da concessionária danifiquem os equipamentos internos do condomínio.

Ao final, o gerador sai de funcionamento e retorna à alimentação através da concessionária.

5.2.2. Contingência – Mesa de Operações

Os *traders* possuem *softwares* de acompanhamento de mercado em seus computadores portáteis e em seus smartphones, bem como acesso a seus endereços de e-mail corporativos e ferramentas profissionais de chat, podendo trabalhar de suas casas. Além disso, há espaço físico em todas as sedes para acomodar a equipe necessária para dar continuidade à gestão e aos procedimentos necessários de controle e acompanhamento dos negócios, caso um dos escritórios tenha de ser evacuado.

5.3. Plano de Continuidade Operacional

O Plano é focado na interação entre as pessoas responsáveis, ou "pessoas designadas", para a adoção de medidas preventivas e efetivas relativas a situações extremas — "desastres" — que impossibilitem, temporária ou permanentemente, o funcionamento de algum dos escritórios do Grupo Leste.

Para os fins deste Plano, desastres são todos os eventos, intencionais ou não, que possam causar a impossibilidade sistêmica ou física de funcionamento de um ou mais endereços do Grupo Leste.

6. Cenários de Contingência - Focos de Preocupação e Plano de Ação

Para atendimento às necessidades mínimas de manutenção dos serviços/atividades das Gestoras, foram definidos uma estrutura mínima física, tecnológica e de pessoal, bem como procedimentos que devem ser adotados sempre que uma situação seja caracterizada como contingência às operações das Gestoras.

Com base no levantamento da estrutura das Gestoras relativa à gestão de recursos e no mapeamento de riscos, as Gestoras têm condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações e/ou no caso de falta impactante de Colaboradores ao local de trabalho.

No cenário de contingência, o Coordenador de Contingência deverá acionar este Plano, em caráter imediato, e iniciar também imediatamente a avaliação das causas que geraram a contingência, para providenciar sua solução o mais rapidamente possível, bem como dar início ao efetivo cumprimento dos procedimentos aplicáveis descritos abaixo, devendo comunicar **no menor tempo possível** o ocorrido aos Colaboradores e indicar, nessa oportunidade, o procedimento a ser adotado por cada Colaborador, de acordo com a contingência ocorrida.

O Coordenador de Contingência deverá acompanhar todo o processo aplicável descrito abaixo até o retorno à situação normal de funcionamento, no contexto das atividades desempenhadas pelas Gestoras, e reportar eventuais alterações e atualizações da contingência aos demais Colaboradores.

7. Aspectos Gerais

Este Plano é de uso restrito dos Colaboradores das Gestoras e **não** pode ser divulgado para terceiros, exceto se autorizado pela Equipe de Contingência.

É responsabilidade do Coordenador de Contingência manter este Plano atualizado, bem como realizar a validação **periódica** dos procedimentos nele estabelecidos.

Ainda, o Coordenador de Contingência realizará testes de contingência que possibilitem que as Gestoras estejam preparadas para eventos dessa natureza, proporcionando-lhes condições adequadas para continuar suas operações.

Sendo assim, **periodicamente**, é realizado um teste de contingência para verificar:

(i) Acesso aos sistemas;
(ii) Acesso ao e-mail corporativo;
(iii) Acesso aos dados armazenados;
(iv) Verificação do treinamento aos colaboradores para atuarem como *back-up*; e
(v) Qualquer outra atividade necessária para a continuidade do negócio.

O resultado do teste será analisado como indicador para a regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano.