CL4 CAPITAL

PLANO DE CONTINUIDADE DE NEGÓCIOS

Versão	Aprovadores	Alterações
Outubro 2023	**Mauricio Jonas, Andre Ishii**	
Fevereiro 2025	**Mauricio Jonas, Marcos Carneiro**	

CL4 CAPITAL

SUMÁRIO

PLANO DE CONTINUIDADE DE NEGÓCIOS

1.1. **Objetivo**

O objetivo deste Plano de Contingência e Recuperação de Desastre (o "Plano de Contingência") é estabelecer procedimentos relacionados ao gerenciamento de situações de contingência, incidentes, desastres ou falhas que possam causar impactos nas rotinas operacionais da CL4 e seus Veículos de Investimento ("Eventos de Contingência").

Os Eventos de Contingência são descritos detalhadamente nos manuais e políticas da CL4, conforme aplicáveis, sendo considerados, por exemplo: a interrupção temporária na prestação de serviços de infraestrutura (energia elétrica, acesso à internet, ou outros serviço essenciais), a ocorrência de impedimento no acesso à sede da CL4 (incêndios, interdição e outras catástrofes sobre o prédio onde funciona a empresa), riscos operacionais e riscos de organização que possam afetar a continuidade das atividades da CL4 e dos Veículos de Investimento.

Dentre as atividades críticas à CL4, esse Plano de Contingência se propõe a cobrir:

(i) A contínua execução das rotinas operacionais dos Veículos de Investimento e da gestora;

(ii) A comunicação regular entre Colaboradores, clientes e parceiros, seja mediante e-mail ou telefone;

(iii) O acesso ininterrupto aos sistemas, informações e arquivos licenciados ou de propriedade da CL4.

1.2. **Medidas Preventivas**

A CL4 adota as seguintes medidas preventivas aos possíveis Eventos de Contingência:

A. **Emergências e simulações de incêndio**: Os Colaboradores são obrigados a participar das simulações periódicas de incêndio realizadas pelo condomínio de modo a se familiarizarem com os procedimentos mínimos exigidos para o caso de uma ocorrência que demande a evacuação do prédio.

B. **Circulação de terceiros**: os visitantes são identificados pelo condomínio, e somente permitidos a subir ao escritório da CL4 mediante prévia aprovação de ao menos um dos colaboradores. Ademais, a entrada de colaboradores no escritório é controlada por sistema de biometria e senha, implantando na única entrada disponível em seu escritório.

C. **Avaliação Periódica de Infraestrutura**: a CL4 realiza anualmente, com o auxílio de terceiros prestadores de serviços, a reavaliação dos seus servidores, links de acesso à internet, redundância de serviços, bem como circuitos elétricos e demais serviços do condomínio relevantes a empresa, com vistas a mitigar riscos à continuidade das atividades por ocorrência de falha nas infraestruturas de suporte.

1.3. **Infraestrutura de TI e Disaster Recovery**

A CL4 opera com uma política de redundância, com servidores produção e *storage* duplicados internamente e também replicados em nuvem (serviço One Drive provido pela MS). Assim, há sempre três conjuntos completos de infraestrutura (dois locais e um cloud) disponíveis 24/7 e em operação paralela, de modo que qualquer falha pontual, em qualquer ponto da infraestrutura, é imediatamente substituída em tempo real, em uma estrutura de *seamless integration* que mantém todos os serviços em funcionamento.

Toda essa estrutura tecnológica visa garantir a manutenção do maior tempo de disponibilidade possível ao escritório da CL4. Ademais, a empresa conta com um acordo de serviços com um fornecedor de infraestrutura e segurança de TI disponível 24/7. Esse fornecedor trabalha remotamente sobre quase a totalidade dos problemas e, caso necessário, está comprometido em mandar um técnico ao escritório para suporte, com SLA de 24 horas.

O servidor de e-mail localizado é provido pela Microsoft, em cloud, junto com outras soluções do Office 365, com um domínio local de contingência. O escritório possui redundância no acesso à internet (2 links) e backup de eletricidade (1 nobreak com 1 hora de autonomia). Em adição, sempre há PCs de backup em caso de falha dos equipamentos existentes.

. O acesso remoto aos sistemas e arquivos por parte dos funcionários é feito por uma VPN para evitar que um vazamento de senha possibilite que alguém externo à empresa consiga acessar os sistemas e arquivos.

Além disso, a estrutura de *Disaster Recovery* espelha todos os serviços internos (arquivos salvos 1 vez ao dia, bases de dados 1 vez por dia e acessos e permissões de usuários online) e estão completamente disponíveis por meio de computadores virtuais. Desse modo, os processos-chave (Trading, Compliance, Backoffice e RI) não sofrem qualquer paralização mesmo em caso de desastre.

Todo o ambiente de tecnologia da CL4 é protegido por *firewall* para garantir o máximo de disponibilidade e o tratamento imediato de ocorrências.

Sumário da Infraestrutura:

Sistemas e Bancos de dados	Localizados em servidores locais na sede da CL4, bem como redundâncias em nuvem na Microsoft (One Drive).
Arquivos	Localizados no escritório da empresa situado, com cópias digitalizadas disponíveis no servidor local em regime de espelhamento em tempo real em nuvem Microsoft. Regime de back-up diário em drive local, com histórico e controle de versionamento.
E-mails	Armazenados em nuvem da Microsoft (Office365) com retenção dos últimos 30 dias.
PABX/ Telefonia	Operação com redundância. Há dois prestadores de serviços.

Desktops Virtuais	Disponíveis 4 Desktops Virtuais no datacenter da CL4, os quais encontram-se sempre atualizados e em total compatibilidade com os sistemas operacionais utilizados nas rotinas diárias da Empresa. Disponível, também, o acesso a Desktops Virtuais mediante por VPN, permitindo a plena continuidade das funções críticas inerentes ao negócio no caso de um Evento de Contingência ou Desastre. Para acesso a tais Desktops Virtuais, é necessário tão somente que o colaborador possua um computador (Windows ou Mac) com acesso à Internet, e a VPN Sophos configurada

1.4. **Procedimentos**

Procedimentos durante um Evento de Contingência ou Desastre

Falha de Sistemas:
No caso de um Evento de Contingência que implique na descontinuidade na prestação de serviço atrelados aos sistemas operacionais considerados críticos o Diretor de Gestão de Riscos e Compliance e o prestador de serviço de TI atuarão para reestabelecer o acesso aos referidos sistemas de forma emergencial. Caso tal falha seja decorrente de um Evento de Contingência na qual fique inviabilizado o acesso ao escritório físico da CL4, os colaboradores devem se orientar para que o acesso seja feito remotamente.

Falha de Infraestrutura:
(a) Energia Elétrica: caso haja falha no fornecimento de energia, a CL4 conta com um nobreak com autonomia de 1 hora de bateria, que é inicializado automaticamente na ocorrência da queda de energia.

- Principais Ações e Responsáveis: Caso os back-ups de eletricidade elencados acima não funcionem ou sejam insuficientes, o Diretor de Gestão de Riscos e Compliance orientará os colaboradores para que se desloquem até suas casas e deem continuidade operacional aos trabalhos via acesso aos Desktops Virtuais.

(b) Comunicações: a CL4 conta com 2 links de acesso à internet (redundância) para a eventualidade de uma falha na prestação do serviço do provedor de internet e/ou no link de dados e um *firewall* dedicado aos dois links. Da mesma forma, os serviços de telefonia estão provisionados permitindo assim o fornecimento de link de voz ininterrupto.

- Principais Ações e Responsáveis: Caberá ao Diretor de Gestão de Riscos e Compliance a responsabilidade de ativação do script de encaminhamento de chamadas para que os colaboradores tenham acesso integral a ligações feitas aos seus ramais originais, em seus telefones celulares pessoais.

(c) Desastres (Incêndio, inundação, assalto, etc): Eventos de Contingência que impliquem na evacuação e/ou inacessibilidade do escritório físico onde está localizada a sede social da CL4, impossibilitando o acesso aos sistemas de operação da empresa.

- Principais Ações e Responsáveis: Além dos procedimentos padrão de evacuação do edifício e atuação ativa dos brigadistas para salvaguardar os colaboradores da CL4, ficará a cargo do Diretor de Gestão de Riscos e Compliance atuar para viabilizar a ativação do site de contingência, permitindo às áreas críticas e aos colaboradores acesso seguro e integral à rede, aos Sistemas Cobertos, aos seus e-mails e demais recursos mínimos necessários para restabelecimento operacional, sem maiores rupturas.

- Para tanto, a orientação aos colaboradores é de procederem às suas residências ou a um local seguro em que possam, por meio de qualquer computador, acessar as máquinas virtuais via One Drive que ficam disponíveis 24/7.

Procedimentos após Evento de Contingência ou Desastre

Na ocorrência de um Evento de Contingência ou Desastre, será estabelecido um comitê de gerenciamento de crise ("Comitê de Gerenciamento de Crise"), composto essencialmente pelo Diretor de Gestão de Riscos e Compliance e um colaborador nomeado em conjunto por ambos, os quais ficarão responsáveis por:

(i) avaliar os impactos diretos e indiretos sofridos;
(ii) elaborar e implementar um plano de ação para recuperação dos serviços impactados, em especial com vistas a restabelecer as funções críticas da CL4, com a maior brevidade possível;
(iii) comunicar aos demais colaboradores acerca do referido plano de ação e se necessário, convocá-los para reunião presencial para esclarecimento de dúvidas e ponderações acerca das medidas que foram e serão adotadas em tal cenário; e
(iv) atuar para a reparação da estrutura afetada, incluindo, mas não se limitando, conforme o caso, ao reestabelecimento do ambiente, dos sistemas de rede e operacionais, bem como estabelecer metodologias de prevenção à ocorrência de novos eventos de contingência ou desastre com características similares (se e quando possível) mitigando, desta forma, o risco de recorrências.

O Comitê de Gerenciamento de Crise será instaurado e permanecerá atuante até que sanados todos os problemas decorrentes do Evento de Contingência ou Desastre e restabelecidas, em sua integralidade, as funções e atividades da CL4.

Registros de Ocorrências

Caberá ao Diretor de Gestão de Riscos e Compliance o registro em pauta de toda e qualquer incidência que implique na ativação dos procedimentos de contingência descritos neste plano. Constará de tal registro, no mínimo:

- Descrição dos fatos;
- Data e hora (quando aplicável) da ocorrência;
- Descrição das medidas adotadas;
- Data e hora (quando aplicável) do reestabelecimento das condições normais de trabalho;

- Informações adicionais (eventualidades, estragos e afins); e
- Assinaturas do Diretor de Gestão de Riscos e Compliance e de um outro sócio.

As pautas de registro ficarão armazenadas no diretório de Compliance na rede pelo prazo de cinco anos.

1.5. **Disposições Gerais**

O presente Plano de Continuidade de Negócios da CL4 descreve todos os procedimentos adotados pela nossa instituição em caso de contingências e desastres, visando sempre cumprindo nosso dever fiduciário, sempre com boa fé, diligência e lealdade.

Esse plano será revisado anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo.

*** * ***