GeoCapital

PLANO DE CONTINUIDADE DE NEGÓCIOS E CONTINGÊNCIA

Outubro/2020

FOLHA DE CONTROLE

Informações Gerais

Título	Plano de Continuidade de Negócios e Contingência
Elaborador	Bruna Veiga
Aprovador	Fabio Maeyama
Data da Aprovação	31/10/2020
Data da Próxima Revisão	31/04/2021
Área Proprietária da Política	Compliance e riscos operacionais
Procedimentos e Outros Documentos Relacionados	Instruções nºs 555 e 558 da Comissão de Valores Mobiliários, Código ANBIMA de Regulação e Melhores Práticas de Fundos de Investimentos.

1. Introdução

1.1. O Plano de Continuidade de Negócios ("Plano") tem o objetivo de garantir os processos, informações e contingência necessárias para evitar a perda ou inabilidade da Geo Capital Gestora de Recursos Ltda., inscrita no CNPJ 19.331.654/0001-26 ("Geo Capital").

1.2. O presente Plano também servirá como base para ativar a contingência planejada para cada situação bem como auxiliar na resolução de eventuais problemas causados por: paradas inesperadas, falta de energia, inacessibilidade física, virtual, perda ou destruição total/parcial de equipamentos e/ou problemas de disponibilização de serviços.

1.3. Fica eleito o sócio Fabio Maeyama, Diretor da Geo Capital, como responsável pelo disposto, em atendimento do disposto na Instrução CVM nº 558, artigo 4º, inciso IV, estando este devidamente registrado no estatuto da empresa.

2. Plano de Continuidade de Negócios

2.1 A Continuidade de Negócios é um processo abrangente que identifica ameaças potenciais inerentes aos negócios e os possíveis impactos nas operações provenientes de tais ameaças. Fornece uma estrutura para que se desenvolva uma capacidade organizacional que seja capaz de responder efetivamente e proteger os interesses das partes envolvidas, reputação, marca da organização e suas atividades de valor agregado.

2.2 A Continuidade de Negócios contempla o gerenciamento da recuperação dos negócios em caso de interrupção, e gestão de todo o Plano de Continuidade de Negócios por meio de treinamentos, testes, revisões e manutenções, a fim de garantir que o plano de continuidade de negócios esteja atualizado e operacional. Por razões que podem fugir do controle interno, um evento crítico pode resultar na sua impossibilidade de cumprir algumas ou todas as obrigações do negócio. Este risco potencial requer o estabelecimento de planos de contingência e retomada dos negócios que levem em conta diferentes tipos de cenários plausíveis aos quais pode potencializar vulnerabilidades, cabíveis às características de complexidade e tamanho das suas operações.

2.3 Para todos os efeitos, fica estabelecido que o responsável pela coordenação, testes e atualização do Plano será o Diretor de Controles Internos e Gestão de Risco e demais membros estabelecidos no Anexo I.

2.4 Todos os Colaboradores da Geo Capital devem conhecer o presente Plano e suas alterações. Caso a Geo Capital entenda ser necessário ou algum Colaborador manifestar interesse sobre qualquer um dos temas pertinentes, treinamento específico poderá ser fornecido.

3. Escopo

3.1. O escopo foi adaptado às necessidades da Geo Capital levando-se em conta a estratégia de investimento, criticidade das atividades, riscos envolvidos e impactos. Pautada pelos deveres de diligência e cuidado e pela respeitabilidade que norteiam a condução dos seus negócios, o presente Plano se baseia no disposto no Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA") e Instrução CVM nº 558 de 2015, para prevenir e lidar com eventos com maior possibilidade de ocorrência, buscando mitigar os riscos nos pontos de vulnerabilidade da sua estrutura de tecnologia.

3.2. Previamente, é necessário garantir a identificação das interdependências entre as instalações, equipamentos e processos de negócios da Geo Capital; o levantamento das diferentes atividades e identificação daquelas com alto interesse estratégico e/ou aquelas com elevado potencial de risco financeiro, físico ou operacional; listagem das instalações, equipamentos, fornecedores, contratados que podem representar dificuldades ou restrição à aplicação deste plano; e verificação da adequação dos meios preventivos e de proteção às características da operação e de negócio.

3.3. Para a continuidade do negócio, serão analisados os seguintes quesitos:

i. Instalações: acesso físico ao prédio e/ou escritório
ii. Equipamentos: utilização, manutenção e troca
iii. Sistemas e Base de dados: demais controles utilizados nas atividades diárias
iv. Sistemas de comunicação: telefonia, internet, e-mails.

4. Riscos Analisados

4.1. Os potenciais riscos foram analisados para se determinar a prioridade e a respectiva probabilidade de ocorrência.

4.2. Como critério de avaliação, foram determinadas notas indicativas (baixo = 1, médio = 2 e alto = 3) para qualificação da probabilidade e impacto.

4.3. A soma dos indicadores resultou na prioridade do risco, sendo que para os riscos que afetam as atividades críticas da empresa, foram elaborados os planos de contingências com os seus respectivos responsáveis.

4.4. A Geo Capital mantém a identificação atualizada de seus principais processos de negócios, de forma que em caso de ocorrência de contingências seja possível retomar as operações com os menores custos de transação e perdas de recursos humanos, físicos, tempo e materiais possíveis.

4.5. Para a retomada célere e eficaz das operações após uma contingência, a Geo Capital mantém procedimentos que a permitem a utilizar alternativas de dentro ou fora das instalações físicas do escritório para substituição de equipamentos danificados, manter o gerenciamento do pessoal e os procedimentos das operações administrativas mesmo durante os efeitos da contingência, retornar definitivamente a utilização das instalações de sua sede após a ocorrência da contingência; e avaliar as perdas da interrupção dos negócios.

4.6. Os Colaboradores são responsáveis por comunicar ao Responsável por Compliance toda e qualquer situação que possa, ainda que potencialmente, dar origem a uma situação que possa levar a ativação dos procedimentos indicados neste Plano. A ativação dos procedimentos descritos neste Plano ficará a critério e será de responsabilidade do Responsável por Compliance.

4.7. A área de Compliance é responsável pela prevenção de perdas e implementação do Plano, podendo ser elencadas outras, caso necessário. Eventuais comunicações para a Área de Compliance devem ser enviadas para: compliance@geocapital.com.br

4.8. Em qualquer hipótese de impossibilidade de utilização da sede da Geo Capital, o escritório de contingência deverá ser acionado imediatamente. Caso a impossibilidade de utilização seja constatada após horário comercial, o escritório de contingência deverá ser acionado no dia útil seguinte.

5. Ativação, Coordenação e Execução do Plano de Contingência

5.1. A Ativação, Coordenação e Execução do Plano será responsabilidade do Diretor de Controles Internos e Gestão de Risco e na sua ausência os analistas de Operações ("*Backups*").

5.2. Uma vez detectada a necessidade de ativação do Plano, seja por comprovação do Diretor de Controles Internos ou por qualquer Colaborador da Geo Capital, fica o Diretor de Controles Internos responsável pela comunicação com demais sócios e Colaboradores.

5.3. Ficará estabelecido os seguintes responsáveis e responsabilidades, de acordo com os recursos:

i. Instalações: Observar inacessibilidade ao escritório da Geo Capital.
Responsável: Fabio Maeyama
Backup: Bernardo Veja
Responsabilidades:
   a) Confirmar inacessibilidade
   b) Avisar todos os funcionários da Geo Capital, conforme lista de contingência (anexo).
   c) Verificar necessidade e autorizar para as funções críticas contingenciamento remoto para acesso a e-mails, planilhas, sistemas e pastas.
   d) Monitorar restauração de acesso às instalações físicas e/ou definir novo local.

ii. Equipamentos

Responsável: Fabio Maeyama
Backup: Guilherme Pereira
Responsabilidades:

a) Analisar e confirmar, perda ou problema técnico com equipamento.
b) Comunicar os funcionários da Geo Capitalimpactados pela indisponibilidade.
c) Comunicar empresa prestadora de serviços para análise e reposição.
d) Avisar diretores da Geo Capitalpara aprovação de compra de novo equipamento.
e) Autorizar para as funções críticas contingenciamento remoto.
f) Monitorar restauração e transição para novo equipamento.

iii. Sistemas
Responsável: Fabio Maeyama
Backup: Guilherme Pereira
Responsabilidades:

a) Analisar e confirmar, indisponibilidade ou perda do sistema.
b) Comunicar os funcionários da Geo Capital impactados pela indisponibilidade.
c) Comunicar empresa prestadora de serviços para análise e restauração.
d) Autorizar para as funções críticas contingenciamento remoto.
e) Monitorar restauração e transição de processos de contingenciamento.

6. Contingência

6.1. A seguir listaremos as contingências criadas para os quesitos listados no escopo, são eles conforme classificação estabelecida:

i. Instalações
Probabilidade de ocorrência: Alta
Impacto: Médio
Risco Potencial: Limitação no acesso físico a Geo Capital ou interrupção do fornecimento de energia, limitando o acesso a dados e sistemas necessários para gestão, atendimento e controles.
Mitigação: Todos os dados e e-mails da Geo Capital são armazenados em "nuvem" e possuem sincronização on-line, portanto acessíveis de acordo com o perfil de cada usuário, remotamente e com padrões de segurança sendo o acesso e utilização rastreáveis e auditáveis. O prédio atual onde se encontra a Geo Capital, possuir gerador independente para energizar os andares de forma autônoma e todas as máquinas contam com "no break" capazes de evitar surtos e/ou pico ou falta de energia.
Contingência: Em situação de contingência, os dados podem ser acessados através de *home office* e através de dispositivos móveis, com autorização do Compliance.

ii. Equipamentos
Probabilidade de ocorrência: Média

Impacto: Médio

Risco Potencial: Perda temporária ou permanente de capacidade de utilização dos equipamentos da Geo Capital.

Mitigação: Todos os dados e e-mails da Geo Capital são armazenados em "nuvem" e possuem sincronização on-line, portanto acessíveis de acordo com o perfil de cada usuário, remotamente e com padrões de segurança sendo o acesso e utilização rastreáveis e auditáveis. Adicionalmente, temos um notebook que pode ser usado como *backup* de computadores.

Contingência: Em situação de contingência, os dados podem ser acessados através de *home office* e através de dispositivos móveis. Vale ressaltar que o nível simplificado das demandas atuais de equipamentos e infraestrutura, torna a sua reposição possível em menos de 24hs.

iii. Sistemas e Base de dados

Probabilidade de ocorrência: Baixo

Impacto: Médio

Risco Potencial: Limitação de acesso por perda de conexão ou perda de dados disponíveis.

Mitigação: A Geo Capital utiliza a armazenagem de dados em "nuvem" que possuem certificação ISO 27001, SOC 2/3 e FISMA, sendo os *data centers* monitorados 24 (vinte e quatro) horas com redundâncias para garantir o serviço ininterrupto inclusive com geradores independentes de energia. Adicionalmente, a Geo Capital possui redundância no link de internet (Vivo e Net) para garantir o acesso à internet.

Contingência: Em situação de contingência, os dados podem ser acessados através de *home office* e através de dispositivos móveis. Vale ressaltar que o acordo de serviços com o provedor de acesso (*Google for Work)* garante 99,9% de disponibilidade aos serviços de acesso a sistemas e e-mail.

7. Verificações da estrutura de tecnologia

7.1. Semestralmente, a equipe de Tecnologia da Informação realizará e coletará evidências que comprovem:

i. Verificação dos "*no breaks*", funcionamento e tempo de carga até o gerador do prédio entrar em operação;
ii. Acesso a sistemas através de ambos links de internet (Vivo e Net);
iii. Acesso aos dados armazenados externamente;
iv. Acesso remoto das principais atividades utilizadas por cada área;
v. Verificação e manutenção de lista atualizada de telefones, para eventual comunicação de contingência.

7.2. A Geo Capital tem duas estratégias implementadas para a continuidade do negócio em caso de desastre ou interrupção das instalações do escritório localizado na cidade de São Paulo, com base na sua peculiaridade de negócios, processos e complexidade onde as pessoas se encontram:

i. O escritório está operacional porém sem acesso físico: a estratégia é recuperar as operações através do acesso remoto a partir do computador pessoal de cada pessoa; ou

ii. O escritório não está operacional: a estratégia é recuperar as operações através do acesso remoto em uma posição de desktop disponível no escritório que não sofreu a interrupção. Os escritórios, São Paulo e Rio, estão preparados para assumir como contingência um do outro.

7.3. Semestralmente, a equipe de Compliance realizará o *Call Tree Test*, que se trata enviar uma mensagem via *WhatsApp* para testar a capacidade e a agilidade de contato com cada um dos colaboradores da Geo Capital em caso de urgência eventual

7.4. Por isso, a equipe de Compliance terá armazenados sobre cada Colaborador:

i. Endereço Completo;
ii. Telefone Residencial;
iii. Telefone Celular;
iv. Meio de transporte principal para chegar ao trabalho;
v. Meio alternativo de transporte para chegar ao trabalho (meio utilizado caso o transporte principal esteja indisponível).

7.5. Através do *WhatsApp* (principal meio de comunicação), será testada a agilidade e a capacidade de retorno dos Colaboradores. Caso algum membro não puder ser localizado dentro de 24 (vinte e quatro) horas, os demais meios de comunicação serão utilizados com base nas informações atuais.

7.6. Ao final do teste, os retornos promovidos por cada Colaborador serão registrados e a área de Compliance elaborará um relatório com o resultado final a respeito da capacidade de contato com cada Colaborador.

7.7. O objetivo deste teste é garantir que será possível entrar em contato com todos os Colaboradores da Geo Capital e tomar as providências necessárias. Tal iniciativa se fará necessária em eventos inesperados como:

i. Incêndio;
ii. Inundação;
iii. Roubo;
iv. Bloqueios / Problemas com administração do edifício;
v. Ameaça de bomba;

vi. Falha grave no link de internet e sua redundância;
vii. Problemas de Hardware ou Software;
viii. Queda de Energia por período prolongado.

7.8. A Geo Capital também conta com o sistema 3CX Phone System, que permite que as ligações de saída passem a ser feitas a partir de telefone externo, em um eventual problema nos troncos de comunicação do escritório.

7.9. A Geo Capital também utiliza os serviços do Google Drive, serviço de armazenamento e sincronização de arquivos, para garantir o armazenamento automático dos documentos e materiais internos.

8. Revisão

Esta Política deverá ser revisada e atualizada semestralmente, ou em prazo inferior, caso necessário, em função de mudanças legais/regulatórias ou complementações.

ANEXO – LISTA DE CONTATOS PARA PLANO DE CONTINGÊNCIA

GEO

Nome	Telefone
Fabio Maeyama	+55 11 99900 6406
Guilherme Pereira	+55 19 98179 6492
Bernardo Vega	+55 11 999616321
Grabriela Cruz	+55 11 96433 0870

Suporte TI e Administração predial

Nome	Telefone	Email
Marcia – Administração Edificio Hungria	+55 11 95500 7354	quadrahungria@fmg.net.br]
WTI Informatica	+55 11 98175 4974	wagner@wti.serv.com