vinland
CAPITAL

Manual de Compliance, Ética e Controles Internos

Data da Atualização: 31/01/2023

Versão: 2023-01

Aprovado por: Ricardo Garcia (diretor)

E Andre Laport (diretor)

Data da Aprovação: 31/01/2023

VINLAND Capital Management
Gestora de Recursos Ltda.

VINLAND Capital Management International
Gestora de Recursos Ltda.

VINLAND Capital Management Crédito Privado
Gestora de Recursos Ltda.

Parte 7
Plano de contingências e continuidade dos negócios

1. Introdução

O objetivo do Plano de Contingência e Continuidade dos Negócios ("BCP") é possibilitar que a Vinland continue com as suas operações e serviços essenciais mesmo nos cenários de crise.

O presente documento define os procedimentos que deverão ser seguidos pela Vinland, no caso de contingência, de modo a impedir a descontinuidade operacional por problemas técnicos. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da Vinland sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

O BCP prevê ações que durem até o retorno à situação normal de funcionamento da Vinland dentro do contexto de seu negócio.

1.1. Cenários de Crise

A Alternative Investment Managment Association (AIMA) lista em seu documento "Business Continuity Management for Hedge Fund Managers – version June 2012" 24 (vinte e quatro) possíveis cenários de crise:

1. Explosão em uma grande área;
2. Fogo;
3. Falta localizada de energia;
4. Explosão localizada;
5. Inundação;
6. Falha de circuito / terminal;
7. Explosão na vizinhança;
8. Pandemia;
9. Falha de hardware;
10. Bomba radiológica;
11. Clima extremo;
12. Vírus / hackers;
13. Guerra ou insurreição civil;
14. Interrupção de transportes;
15. Roubo / sabotagem;
16. Alerta de segurança;
17. Acidentes (dentro ou fora do escritório);
18. Falha no sinal de Telecom (internet e/ou voz);
19. Vazamento de gás;
20. Eletrocussão;
21. Falha no hardware de Telecom;
22. Terremoto;
23. Falta geral de energia (apagão); e
24. Falha na rede de celular.

Uma vez que ocorra algum incidente parecido com estes 24 (vinte e quatro) cenários ou algo que chame a atenção do Colaborador, o líder do BCP – que é o Diretor de Compliance, Risco e PLD ou na ausência deste o seu back-up – deverá ser imediatamente comunicado. (Ver item 4 – lista de contatos de emergência).

1.2. Desdobramentos

A lista de cenários apresentadas em no item 1.1 não tem a pretensão de ser definitiva. Além disto, cenários de crise são por definição imprevisíveis. No entanto os cenários acima geralmente levam a combinação de um ou mais dos desdobramentos abaixo:

(i) Perda de Acesso ao Prédio: significa que todos os colaboradores e contratados da Vinland que estiverem no prédio no momento do incidente deverão evacuá-lo e quem estiver fora não poderá entrar.

(ii) Perda de Pessoal: afeta os Colaboradores e prestadores de serviços da Vinland. Inclui ferimentos, doenças, morte e incapacidade de chegar no escritório (ou potencialmente trabalhar de casa).

(iii) Perda de Infraestrutura de TI: inclui falha parcial ou completa da rede de TI, incluindo hardware e softwares essenciais. O fator-chave é envolver os prestadores de serviços assim que possível para instaurar os sistemas de back-up.

(iv) Perda de Infraestrutura de Telecom: inclui falha parcial ou completa da rede de telecomunicações, incluindo equipamentos, telefones fixos, celulares e a internet).

(v) Perda de Energia Elétrica: Falta de energia devido a apagões ou interrupção da rede elétrica devido a chuvas e/ou quedas de árvores.

2. Gestão da Crise, Recuperação e Retomada

Uma vez que o líder do BCP foi acionado devido a uma potencial crise, caso seja possível ele convocará (pessoalmente ou via call-tree) os colaboradores-chave da Vinland para formar o comitê de crise e avaliar conjuntamente a situação e próximos passos.

Na impossibilidade de decisão em conjunto – devido a situação onde a pressão é extrema – o líder do BCP poderá tomar decisões sozinho sobre os próximos passos para gerenciar a crise.

DS RG DS

Existem geralmente três etapas a serem percorridas após a ocorrência de um evento: (i) Gestão da Crise; (ii) Recuperação e (iii) Retomada.

2.1. Gestão da Crise

Etapa Inicial: engloba vários aspectos e decisões fundamentais a serem tomados imediatamente após o incidente:

1.1. Avaliação dos impactos: o foco da reunião do time de crise deve ser:

1.1.1. Entender o que aconteceu;

1.1.2. Quais são as consequências imediatas e gravidade da situação;

1.1.3. Como manter os Colaboradores a salvo; e

1.1.4. O que nós devemos fazer e decidir pela formalização ou não da crise (Em caso afirmativo os próximos passos são seguidos):

1.2. Comunicação ao restante dos Colaboradores;

1.3. Evacuação do prédio coordenada em conjunto com a administração predial;

1.4. Acionar assistência médica imediata se necessário;

1.5. Notificação dos serviços de emergência (bombeiros, polícia, SAMU) se necessário;

1.6. Condução de chamada para ver os Colaboradores e visitantes presentes;

1.7. Retomada da reunião do comitê de crise;

1.8. Realocação dos Colaboradores:

1.8.1. Quem trabalhará por meio de home office e quem vai para o site de contingência;

1.8.2. Combinar como serão as próximas comunicações (telefone, WhatsApp);

1.9. Notificação de parceiros-chave estratégicos: prestadores de serviços de TI e Telecom (Tecnoqualify); prime brokers, administradores dos fundos, contador etc. Tomar cuidado para manter a consistência da comunicação ao informar terceiros. Apenas os Colaboradores autorizados a falar em nome da empresa serão responsáveis por esse aspecto (ver lista de autorizados no Código de Ética).

1.10. Iniciar a redundância de TI (caso seja aplicável) em conjunto com a Tecnoqualify; e

1.11. Redirecionamento das linhas de telefone para os celulares (caso seja aplicável)

Recuperação de Desastre – TI: após determinar a necessidade ou não de redundância de TI, o comitê de crise deverá atuar em conjunto com a Tecnoqualify para garantir que qualquer aplicativo e hardware críticos continuem a operar via redundância/back-up. Isto inclui:

- acesso ao servidor de e-mails;
- acesso aos principais servidores (aplicativos e arquivos)
- acesso aos serviços replicados no cloud Azure (arquivos)
- acesso remoto aos sistemas.

Telecom: caso a redundância de Telecom seja necessária, o provedor deve ser instruído a desviar linhas de dados/e-mail.

Comunicação Externa: a gestão de relacionamentos externos durante uma interrupção das atividades normais é crítica para o curto e médio prazo da Vinland. No curto prazo os prestadores de serviços críticos devem ser avisados para que eles adaptem os seus processos para a nova circunstância. No longo prazo, prover uma comunicação clara, pontual e consistente a clientes, distribuidores e contrapartes fortalece a confiança na organização

O Comitê de Crise produzirá um script padrão para comunicar interna e externamente (demais prestadores de serviços, clientes, dentre outros). É muito importante que a comunicação externa seja consistente uma vez que confusão poderá resultar em perda de confiança.

Caso algum Colaborador (que não esteja autorizado a falar em nome da Vinland) seja questionado por terceiros, o Colaborador deverá direcionar o terceiro para alguém que esteja autorizado.

2.2. Recuperação

A fase de recuperação começa após a crise inicial ter sido contornada, ou seja, o Colaboradores já foi recolocado, a redundância de TI acionada e terceiros-chave notificados. A fase de recuperação é composta das subfases a seguir:

Comunicação Interna: call diário de acompanhamento do Comitê de Crise e outro call com os demais membros da Vinland. Ambos devem ser minutados pelo líder do BCP e conter as tarefas de cada área (atividade/responsável/prazo);

Ações Iniciais de Recuperação:

1.1. Comitê de Riscos e Compliance: deverá se reunir assim que possível para avaliar o impacto do incidente nos diversos riscos (mercado, crédito, operacional, dentre outros) e caso necessário tomar as devidas ações;

1.2. Comitê de Investimentos: o CIO e o COO devem juntamente convocar uma reunião para verificar se todas as informações necessárias ao portfólio estão seguras. Dados faltando ou corrompidos devem ser comunicados ao Comitê de Crise. A Área de Investimentos e o COO devem decidir se decisões de investimento são requeridas embora o trading discricionário deva ser minimizado de acordo com as novas condições operacionais da Vinland.

1.3. Área de Operações (Middle Office): este time deverá continuar a manter informados o administrador fiduciário do fundo, prime brokers e outros contrapartes operacionais-chave.

Cobertura de funções críticas: todas as áreas funcionais deverão ter previamente identificado as suas atividades críticas e o seu pessoal-chave necessário. Estas funções deverão ser conduzidas com qualquer problema sendo escalado ao Comitê de Crise.

Data Management:

1.1. Migração dos trabalhos conduzidos externamente durante a crise para os sistemas essenciais (ou back-up)

1.2. Back-up de dados em ambiente de Recuperação ou em Redundância no Cloud.

Comunicação Externa: stakeholders-chave externos devem ser atualizados regularmente.

Cenários de Retificação/ Contingência

1.1. Acesso ao prédio: no caso de o prédio ter sido evacuado, ou o acesso a ele estar negado, é provável que documentos ou hardware importantes estejam dentro deste.

1.2. Buscar acomodação alternativa: no caso de o prédio ter sido gravemente danificado ou destruído e a reocupação não seja possível a médio prazo (ou nunca mais).

2.3. Retomada

A terceira fase é a transição entre estar trabalhando em "modo recuperação" para voltar ao modo normal (business as usual). Os temas cobertos por esta fase são dependentes do evento ocorrido, mas podem incluir:

- Como a Vinland retomará suas atividades em conformidade com as regras internas e da regulamentação?
- Algum sistema necessita ser reconstruído?
- A Vinland irá mudar para um novo escritório?

3. Redundâncias e Contingências

Em caso de eventos de crise, a Vinland possui contingências e redundâncias de forma a permitir a continuação de suas atividades mesmo em condições adversas.

3.1. Redundância de TI / Back-up de Arquivos

Backup Server: o servidor possui software de back-up, responsável pela realização de back-up predefinido pela política da Vinland.

O Ambiente tem uma réplica em Cloud do Ambiente local no serviço da Microsoft Azure sendo acessado com VPN SSL pelos usuários.

A Vinland disponibiliza em seus servidores o serviço de backup e restore de arquivos, que tem o intuito de garantir a segurança das informações, a recuperação em caso de desastres e garantir a integridade, a confiabilidade e a disponibilidade dos dados armazenados.

Os Backups são feitos através da ferramenta de backup do Windows 2019 Server e Azure Backup Storage em cloud, com agenda diária das pastas de dados de toda a empresa, devendo ser usado em casos em que não é mais possível a recuperação do arquivo danificado ou perdido.

O serviço de e-mail da Vinland é garantido por parceiro Microsoft que provém suporte 24/7, serviço de anti-spam, anti-vírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A Vinland possibilita o acesso remoto de todas as mensagens pelos colaboradores.

O serviço de e-mail da Vinland é garantido por dispositivo de segurança que executa funções de firewall e antivírus no nível do roteador. Além disso, Anti-virus (software) é ativado em cada computador individual na rede de escritório.

3.2. Redundância de Infraestrutura (Telecom, Internet e Energia)

Telefonia: a Vinland conta com 02 tipos de links de Telefone, sendo 2 (duas) linhas analógicas e 1 (um) Link E1. Em caso de falhas nas linhas telefônicas, os colaboradores da Vinland ainda possuem celulares que podem substituir a telefonia fixa.

Internet: o acesso à internet é disponibilizado por 2 (duas) links de velocidade de 50 (cinquenta) e 150 (cento e cinquenta) mbps no link dedicado (Algar e Mundivox) e 2 (dois) links ADSL de 100 (cem) mbps link VIVO e NET.

Energia: em caso de falha de fornecimento de energia, a Vinland possui nobreak para suportar o funcionamento de seus servidores, rede corporativa, telefonia e 2 (duas) estações de trabalho (desktops) para a efetiva continuidade dos negócios durante 2 (duas) horas. Após este período caso não retorne a energia a equipe será direcionada para um acesso na estrutura cloud.

O sistema de contingência de energia no condomínio possui um gerador que entra em até 5 (cinco) minutos em caso de falta de energia da operadora.

Teste de no-break realizado 2 (duas) vezes por ano.

3.3. Site de Contingência e Home-Office

Em caso da perda de acesso ao escritório da Vinland, os colaboradores poderão acessar o site de contingência virtual e trabalhar de casa com acesso VPN (home-office).

O site de contingência está no Microsoft Azure com acesso pela VPN tipo SSL sendo ativo micros virtuais com os sistemas da empresa.

O site de contingência fica disponível 24x7 sendo acessado pelos os usuários que necessitam estar em home office, assim validando diariamente a estrutura.

No site de contingência virtual, a Vinland possui 02 (dois) Desktops virtuais dedicados e devidamente autorizados. Estes desktops possuem a configuração dos aplicativos essenciais da Vinland. Ainda, o ambiente cloud é composto por duas pontas com acessos segregados, sendo:

1. Microsoft Azure com as configurações de Server Domain Controller, File Server e Desktops de contingência;

2. Microsoft Azure com as configurações de System Database;

Os ambientes são configurados para se replicarem automaticamente, independente se o uso for o principal local ou o de contingência cloud. A Vinland também conta com acesso remoto via VPN à sua rede de dados e alguns aplicativos para os Colaboradores que optarem pelo home office. Tal acesso encontra-se disponível a todos os Colaboradores autorizados pelo Diretor de Compliance, Risco e PLD.

DS RG DS

As informações dos portfólios além de estarem nos sistemas internos da Vinland são disponibilizadas diariamente pelo administrador fiduciário, que também informará qualquer movimentação no passivo dos fundos de investimento para adequação do caixa dos fundos de investimento.

4. Risco de Pessoal

O ambiente pessoal envolve todos os colaboradores e prestadores de serviços existentes na Vinland relacionados à atividade de gestão de recursos. Suas funções devem atender às necessidades de funcionamento da Vinland em situações consideradas de normalidade bem como em situações consideradas de contingência.

Este BCP visa atribuir prioridades e responsabilidades à equipe da Vinland de forma a impactar o mínimo possível em suas atividades em situação de contingência.

O principal ponto identificado de risco é a não existência de um back-up de atividades executadas por um determinado funcionário. Esse risco, no entanto, não é considerado como relevante pois a estrutura da Vinland já conta hoje com a definição e treinamento dos funcionários para atuação como back-up das funções e responsabilidades de seus colegas na Vinland. Tal medida já existe e é praticada regularmente quando, por exemplo, um determinado colaborador se ausenta da Vinland (por férias ou licença) e suas atividades continuam sendo executadas pelo seu back-up designado.

5. Lista de Contatos de Emergência

A Vinland desenvolveu uma lista de Contatos de Emergência que inclui os nomes, telefones, endereços de e-mail dentre outras informações críticas para o negócio. Esta lista inclui colaboradores-chave, distribuidores de fundos, clientes de carteiras administradas, contrapartes prestadoras de serviços essenciais dentre outros contatos. Esta lista será revista e atualizada, anualmente, sendo divulgada internamente.

6. Revisão Anual, Atualização, Treinamento e Testes

6.1. Revisão Anual e Atualização

O BCP deverá ser revisado anualmente e atualizado sempre que for necessário. Cada revisão deverá ser aprovada pelo Diretor de Compliance, Risco e PLD e as cópias do plano revisado deverão ser distribuídas a todos os Colaboradores da Vinland. O BCP também será revisto caso aconteça alguma das situações abaixo:

- Mudanças materiais – organizacionais – no negócio da Vinland;
- Mudanças de pessoal;
- Mudança de endereço do escritório da Vinland ou abertura de um escritório adicional;
- Introdução de novos processos ou alteração dos existentes;
- Upgrade ou alterações na infraestrutura de IT e/ou sistemas; e
- Mudança de prestador de serviço relevante.

6.2. Treinamento e Testes

O treinamento dos Colaboradores em relação ao BCP ocorre fundamentalmente com os procedimentos de teste. No caso de um novo Colaborador a Área de Compliance e Risco lhe apresentará a última versão do BCP.

O BCP deverá ser testado anualmente para garantir que ele funcione em caso de necessidade. Os principais testes são elencados a seguir:

Call Tree: o líder do BCP começará o teste fora do horário comercial - sem aviso prévio - transmitindo uma palavra código para os participantes do call tree. No dia seguinte, todos os participantes deverão reportar a palavra-código transmitida. Este teste avalia a viabilidade do call tree e se os números de telefone foram corretamente registrados.

Conectividade Remota e Site de Contingência: todo o Colaboradores que possuir acesso remoto via VPN (Virtual Private Network) deverá se logar na rede da Vinland a partir de casa e checar se todos os sistemas essenciais e acessos funcionam perfeitamente. Um colaborador da equipe de Gestão e um de Middle-Office/Riscos deverão efetuar os testes através dos notebooks localizados no site de contingência.

Redundância de TI: durante um final de semana, o provedor de serviços de TI (Tecnoqualify) irá acionar o sistema back-up e todo o Colaboradores tentará logar no sistema testando as aplicações essenciais. Posteriormente – no mesmo final de semana – o sistema principal/primário será acionado novamente, para testar o processo de retomada.

Redundância de Telecom: durante um final de semana, todas as linhas fixas de telefone serão testadas e então estes serão testados através de um call tree para telefones fixos. Posteriormente – no mesmo final de semana – as linhas fixas serão reativadas e testadas como parte do processo de retomada.

Redundância de Energia (Nobreaks): durante um final de semana, a energia será desligada e o nobreak interno entrará em funcionamento. Os acessos e os sistemas essenciais deverão ser checados. Posteriormente – no mesmo final de semana – a energia será reativada e os acessos novamente testados como parte do processo de retomada.

Teste Completo: durante um dia útil a ser combinado, a estrutura primária de TI será desligada pela manhã e o sistema de back-up entrará em vigor; os telefones fixos serão desviados para os celulares e nenhum Colaborador (incluindo prestadores de serviços de TI) serão permitidos no escritório. Todo os Colaboradores trabalharão de casa ou do site de contingência priorizando as atividades essenciais da análise de impacto no negócio. O time de Crise gerenciará ativamente o teste organizando conference calls conforme planejado. No final do dia, os sistemas primários de TI e a telefonia fixa serão restaurados. No dia seguinte, todo os Colaboradores deverão checar se os arquivos foram propriamente salvos nos servidores primários. Este teste também verificará se as atividades chaves foram corretamente identificadas dentre outros.

DS RG DS

7. Obrigações dos Colaboradores da Vinland em relação ao BCP

O BCP requer o engajamento de todos os Colaboradores da Vinland, os quais deverão obrigatoriamente:

- Manter uma versão impressa atualizada do BCP em casa e no escritório;
- Ter programado no seu celular os números dos telefones do líder do BCP, seus colegas imediatos e do seu supervisor;
- Ter o número do conference call do BCP programado no celular e a senha de acesso ao conference room facilmente acessível;
- Testar periodicamente o acesso aos sistemas primários e back-ups via VPN (aqueles que tiverem acesso e estrutura computador/internet para o home-office);
- Manter uma política de mesa limpa (clean desk policy): no caso de um roubo ou incêndio, os papéis guardados ficam muito mais seguros do que aqueles deixados soltos;
- Os colaboradores que gerenciem ou tenham relacionamentos com prestadores de serviços também devem manter programados os contatos destes no celular.