PLANO DE CONTINGÊNCIA

VELT PARTNERS

1. Introdução

1.1. Objetivo

A VELT Partners Investimentos Ltda. ("**Empresa**" ou "**VELT Partners**") elaborou este plano de contingência e recuperação de desastre (o "**Plano de Contingência**") com o objetivo de estabelecer os procedimentos adequados ao gerenciamento de situações de contingência, cenários de incidentes, desastres ou falhas que causem impacto nas rotinas operacionais da empresa como um todo ("**Eventos de Contingência ou Desastre**") com vistas a assegurar à VELT Partners e seus colaboradores a plena continuidade operacional das atividades da empresa, a todo tempo e sob qualquer circunstância.

São exemplos de Eventos de Contingência ou Desastre: suspensão total ou interrupção temporária na prestação de serviços por provedores de energia, acesso à internet, serviços de telefonia, etc., catástrofes naturais que impeçam o acesso ao prédio, interdição do prédio onde funciona a sede da VELT Partners por qualquer motivo, inclusive em cenários de greves, pane nos sistemas e softwares utilizados pelos Colaboradores da Empresa, perda de arquivos por qualquer motivo, dentre outros.

Dentre as funcionalidades críticas à VELT Partners a que este Plano de Contingência se propõe a cobrir incluem-se (i) a contínua execução de trades (com a respectiva manutenção das regras de *compliance* aplicáveis), (ii) o desempenho das rotinas operacionais, (iii) a possibilidade de recebimento e troca regular de e-mails (sejam internos ou com contrapartes externas) e atendimento telefônico via PABX além de (iv) acesso/uso ininterrupto aos sistemas, funcionalidades e arquivos utilizados pela Empresa, conforme descritos no item 1.2 abaixo ("**Sistemas Cobertos**"), mesmo em caso de total impossibilidade de acesso ao escritório físico da Empresa.

1.2. Funcionalidades e Sistemas Cobertos

São funcionalidades e Sistemas Cobertos para fins deste Plano de Contingência:

(i) E-mails & Intranet;

(ii) Arquivos

(iii) Sistema de *trade* e *compliance*, controladoria e carteiras – AlphaTools da INOA; e

(iv) Bloomberg

2. Medidas Preventivas

A VELT Partners adota as seguintes medidas preventivas visando a mitigação de eventuais riscos de ocorrências de Eventos de Contingência ou Desastre:

A. **Rota de fuga, sinalização de emergência e simulações de incêndio:** a sinalização das rotas de fuga e colocação da sinalização de emergência é feita em locais estratégicos do escritório da Empresa e facilmente identificáveis. Os colaboradores são ainda, instruídos à se portarem com um padrão de conduta adequado em caso de incidentes com fogo. Neste caso, 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. **Identificação de visitantes / Circulação de terceiros:** com vistas a assegurar um nível de segurança mínimo nas suas premissas, os visitantes são identificados pelo condomínio, e somente permitidos a subir ao escritório da VELT Partners mediante prévia aprovação de um dos colaboradores. Neste mesmo sentido, os visitantes e prestadores de serviços são instruídos a observar o procedimento padrão para circulação dentro do escritório, não sendo permitida sua entrada no salão principal exceto se acompanhado de um colaborador. Ademais, a entrada de colaboradores no escritório é controlada por sistema biométrico implantando na única entrada disponível em seu escritório, evitando-se, assim, o acesso por terceiros que eventualmente tomem posse de crachás de identificação pessoal dos colaboradores (os quais tão somente permitem a entrada no edifício, mas não garantem efetivo acesso ao escritório da Empresa).

C. **Monitoramento do Ambiente Corporativo:** o monitoramento do ambiente corporativo se dá através da instalação de câmeras em locais estratégicos do escritório, permitindo a identificação de quem circula nas suas áreas comuns a todo o tempo, com a respectiva retenção das gravações.

D. **Avaliação Periódica dos Circuitos Elétricos e Instalações Hidráulicas:** a Empresa, através de prestadores de serviços terceirizados, realiza anualmente a reavaliação dos circuitos elétricos e do sistema hidráulico de seu escritório com vistas a mitigar riscos de curto-circuito e rompimento e/ou defeito das instalações hidráulicas (registros, válvulas e pontos de infiltração).

E. **Telefones de Colaboradores:** a Empresa disponibiliza aos seus colaboradores - em sua intranet - o acesso à lista de telefones celulares pessoais de cada um dos demais colaboradores, inclusive para os casos de emergência, facilitando assim a comunicação em cenários de estresse ou emergenciais.

3. Infraestrutura Tecnológica

A VELT Partners é detentora de uma infraestrutura tecnológica robusta. A Empresa opera em 3 datacenters externos em nuvem – Microsoft Azure, AWS e Google Coud, Microsoft Azure possui serviço de geo-redundância em um outro continente e ele é responsável pelos sistemas Alpha Tools da INOA, Sistema de Arquivos (*File Server*) e *backup*, AWS responsável pela nossa intranet e Google Cloud responsável pelo nosso armazenamento para Data Science.

Sistemas e Banco de Dados: O servidor responsável pelo sistema de produção (Alpha Tools) e o serviço de bancos de dados da Empresa estão localizados na Nuvem, com contrato que inclui 99,99% de uptime e geo-redundância – isto é, os sistemas são espelhados, online, em outro datacenter do mesmo fornecedor, localizado em continente diverso. A VELT Partners se conecta até o Microsoft Azure através de VPN criptografada e IP redundante.

Arquivos: O servidor responsável pelo sistema de arquivos (*File Server*) da VELT Partners está localizado no datacenter Microsoft Azure com backups diários pelo sistema de backup do Azure para retenção histórica de 5 anos.

E-mail: O sistema de e-mail também está localizado fora do escritório (Microsoft Office 365), com retenção/armazenamento automático de todos os e-mails por 5 anos. Sendo assim, em caso de um Evento de Contingência ou Desastre, todo o histórico de e-mails estará disponível via *webmail*, o qual conta com mecanismos de *Two Factor Authentication*, e o fluxo de entrada e saída de e-mails não será afetado.

Acesso à rede: Todas as permissões de rede/login/senha são controladas por um *domain controller* no Microsoft Azure. Ou seja, viabilizando desta forma, o acesso remoto à rede com o mesmo login e senha de acesso utilizados no escritório físico. O acesso remoto aos sistemas e arquivos por parte dos funcionários é feito por uma VPN com *Two Factor Authentication*, para evitar que um vazamento de senha possibilite que alguém externo à empresa consiga acessar os sistemas e arquivos.

PABX: Nossa telefonia (PABX e troncos) está também no Microsoft Azure. Todos os ramais se conectam a este PABX por meio de uma VPN IP redundante. Em caso de contingência, os colaboradores da VELT possuem o ramal configurado em seu telefone celular pessoal. Assim há garantia de acesso telefônico total e irrestrito em situações de *Disaster Recovery*. Adicionalmente, vale ressaltar que todas as ligações são gravadas e ficam retidas por 5 anos.

Escritório: O escritório da VELT Partners possui redundância no acesso à internet (3 links), backup de eletricidade (2 nobreaks com 3 horas de autonomia e 4 geradores no prédio) e redundância de firewall. Em adição, há Notebooks de backup disponíveis em caso de falha dos equipamentos existentes. O plano de contingência foi estruturado de forma a garantir a manutenção do maior tempo de atividade possível ao nosso escritório.

Disaster Recovery: A estrutura externa de *Disaster Recovery* (ver abaixo "Estrutura e Plano de *Disaster Recovery*") é sincronizada automaticamente e pode ser acessada em Eventos de Contingência ou Desastre, observados os critérios e procedimentos abaixo definidos.

4. Estrutura e Plano de *Disaster Recovery*

A VELT Partners possui uma estratégia para cenários de desastre composta por (i) back-ups de seus sistemas e (ii) estações de trabalho virtuais para acesso remoto, com sincronismo diário e completamente disponíveis para uso em caso de um desastre físico envolvendo seu escritório.

(i) Back-up de Sistemas: com relação aos sistemas, todos os sistemas de produção da Empresa estão localizados em um datacenter externo da Microsoft em São Paulo, com back-up online para outro datacenter do mesmo fornecedor em continente diverso (geo-redundância). Assim, em caso de um desastre que atinja fisicamente o datacenter principal, os colaboradores poderão imediatamente acessar os sistemas de produção no datacenter de back-up.

(ii) Acesso remoto: com relação ao acesso remoto por colaboradores da VELT Partners a seus computadores, a VELT Partners conta com estações de trabalho virtuais na Nuvem para cenários de contingência. Estas estações de trabalho virtuais destinam-se a atender as principais áreas críticas da Empresa, com funções que são *time sensitive* e não podem parar ("Estações de Trabalho Virtuais"). Os Sistemas Cobertos ficam atualizados nestas Estações de Trabalho Virtuais, a todo o tempo, formando um ambiente de *Disaster Recovery* ("DR"). Sempre que instalado um novo sistema ou uma versão de sistema atualizada no ambiente de produção, o mesmo procedimento é replicado no ambiente de DR mantendo, desta forma, os computadores de uso diário e os virtuais simultaneamente sincronizados. O acesso a estas estações por parte dos funcionários é feito por uma VPN com *Two Factor Authentication*, para evitar que um vazamento de senha possibilite que alguém externo à empresa consiga acessar os sistemas e arquivos. Da mesma forma, o acesso a e-mails através do webmail, conta com a proteção do mecanismo de *Two Factor Authentication*. Todo o ambiente de *Disaster Recovery* é protegido por firewall.

O acesso ao ambiente de DR é feito através da utilização de mesmo usuário e senha da rede adotados no acesso ordinário de dentro da Empresa, apenas com o adicional de fechamento da VPN com *Two Factor Authentication* com o ambiente, similar ao que já é feito hoje para conexão remota.

5. Procedimentos

5.1. Procedimentos durante um Evento de Contingência ou Desastre

- **Falha de Sistemas:**

No caso de um Evento de Contingência ou Desastre que implique na descontinuidade na prestação de serviço atrelados aos sistemas operacionais considerados críticos – Sistemas Cobertos, e/ou em seus servidores e rede, o CTO atuará para reestabelecer o acesso aos referidos sistemas de forma emergencial, além de ativar imediatamente e disponibilizar na rede em modo redundante. Caso tal falha seja decorrente de um Evento de Contingência ou Desastre na qual fique inviabilizado o acesso ao escritório físico da VELT Partners, os colaboradores são orientados a trabalhar de suas casas, utilizando laptop corporativo conectado à infraestrutura de nuvem da VELT via VPN, ou realizando acesso remoto nas Estações de Trabalho Virtuais.

- **Falha de Infraestrutura:**

(a) Energia Elétrica: caso haja falha no fornecimento de energia, a VELT Partners conta com os seguintes recursos: (i) 2 sistemas de alimentação secundária de energia elétrica (nobreaks) com 3 horas de autonomia de bateria; e (ii) 4 geradores no prédio inicializados automaticamente em caso de queda de energia e com mais de 36 horas de autonomia.

- ✓ Principais Ações e Responsáveis: Caso os back-ups de eletricidade elencados acima não funcionem ou sejam insuficientes, o CTO orientará os Key Users para que se desloquem até suas casas e deem continuidade operacional aos trabalhos utilizando-se dos laptops corporativos, conectados via VPN à infraestrutura na nuvem VELT.

(b) Comunicações: a VELT Partners conta com 3 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. Ademais, todos os ramais se conectam por meio de um PABX que é ligado por meio de uma VPN IP redundante, permitindo assim o fornecimento de link de voz ininterrupto.

- ✓ Principais Ações e Responsáveis: Os celulares pessoais dos Colaboradores são configurados pelo time de TI da VELT, desde o início de seus respectivos vínculos de trabalho, para receberem as chamadas feitas aos seus ramais corporativos.

(c) Controle Ambiental CPD: o ambiente do CPD situado no escritório da VELT Partners é monitorado regularmente para garantir o seu correto funcionamento e a manutenção de temperatura (aproximadamente 21º C).

- ✓ Principais Ações e Responsáveis: O CTO é responsável por monitorar diariamente, inclusive via acesso remoto, as condições mínimas de funcionamento do CPD. Caso haja qualquer intercorrência no ambiente do CPD gerando falha nos mecanismos de controle e/ou alteração de tais condições, o CTO atuará para mitigação das falhas e reestabelecimento de suas funcionalidades, inclusive comunicará à Diretora de Compliance e Gestão de Risco da VELT Partners (nomeada nos termos do seu contrato social) caso verifique que um problema no CPD pode causar falhas acessórias sistêmicas. Neste sentido, o CTO e a Diretora de Compliance e Gestão de Risco atuarão, conjuntamente, para desenvolver um plano imediato de ação. Dependendo do grau de complexidade da falha e por medida de segurança, caberá a Diretora de Compliance e Gestão de Risco orientar os demais colaboradores a procederem à evacuação do escritório, com a devida continuação dos trabalhos de suas casas, utilizando-se do laptop corporativo conectado à infraestrutura na nuvem VELT. Caso isso aconteça, o CTO

solicitará à administradora do escritório que proceda à imediata comunicação dos fatos ao condomínio.

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

- ✓ Principais Ações e Responsáveis: Além do procedimento padrão de evacuação do edifício e atuação ativa dos brigadistas para salvaguardar a vida dos colaboradores da VELT Partners, ficará a cargo do CTO e em sua ausência, da Diretora de Compliance e Gestão de Risco da VELT Partners, atuar para viabilizar a ativação do site de contingência, permitindo às principais áreas críticas e aos colaboradores designados para seu acesso, nos termos acima, 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, através de qualquer computador, acessar as estações de trabalho virtuais que ficam disponíveis na Nuvem, em datacenter no Brasil, seguindo os procedimentos descritos no item 5.2 abaixo.

- ✓ Tempo de Ação: Imediato - quanto antes for a atuação da Empresa e de seus colaboradores, menor será o prejuízo. O CTO da VELT Partners ficará a inteira disposição dos Key-Users para viabilizar os acessos aos Sistemas Cobertos em Eventos de Contingência ou Desastre.

5.2. Acesso ao Ambiente DR

Como todos os Sistemas Cobertos encontram-se na nuvem, Eventos de Contingência ou Desastre e indisponibilidade de acesso ao escritório físico não causam um impacto direto à continuidade dos negócios. Para tanto, contamos com Estações de Trabalho Virtuais pré-configurados que permitem a continuidade imediata das funções mais críticas, conforme melhor detalhado abaixo.

Neste cenário, os colaboradores permanecem com acesso full aos e-mails (incluindo nos aparelhos celulares) e com as ligações para os ramais redirecionadas. Os bancos de dados, sistemas e arquivos estarão no exato estado imediatamente anterior ao Evento de Contingência ou Desastre, bastando o acesso às Estações de Trabalho Virtuais. Os procedimentos para acesso as Estações de Trabalho Virtuais encontram-se detalhados abaixo:

- ➢ Acesso ao DR utilizando Windows 11 / 10
- ➢ Acesso ao DR utilizando Mac

A Empresa disponibiliza o acesso ao ambiente DR para dois grupos segregados de colaboradores, quais sejam:

(I) Key Users – Em um Evento de Contingência ou Desastre, as Estações de Trabalho Virtuais ficam disponíveis primariamente para atendimento às principais áreas críticas para a continuidade do negócio, quais sejam: *Trading, Operations, Compliance* e Relações com Investidores.

(II) Demais Colaboradores: Estações de Trabalho Virtuais adicionais podem ser disponibilizados, subsidiariamente, à área de TI e aos demais colaboradores da Empresa, os

quais podem acessar os arquivos da rede independentemente desta ferramenta, bastando para tanto que acessem o servidor de arquivos via fechamento de uma VPN.

A prioridade de atendimento é para os *Key Users*, seguida de restauração do ambiente de produção e posteriormente, atendimento e acesso aos demais usuários. Em caso de problemas no acesso durante um Evento de Contingência ou Desastre, os colaboradores são orientados a contatar um dos membros do time de TI da Empresa.

5.3. 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 CTO, pela Diretora de Compliance e Gestão de Risco 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 4 funções críticas à Empresa, 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 Empresa.

6. Registros, Treinamentos & Revisões Periódicas

6.1. Registros de Ocorrências

Caberá ao Comitê de Gerenciamento de Crise 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 da Diretora de Compliance e Gestão de Risco e do CTO.

As pautas de registro ficarão armazenadas com a Diretora de Compliance e Gestão de Risco pelo prazo de cinco anos.

6.2. Treinamentos Periódicos

Todos os Colaboradores comparecerão a um treinamento anual sobre este Plano de Contingência (e quando necessário, a reuniões adicionais sobre o tema), que poderá se dar no formato de comunicações internas para conscientização dos Colaboradores. Se for por meio de treinamento, este será elaborado e apresentado pelo CTO sob supervisão da Diretora de Compliance e Gestão de Risco.

6.3. Revisões e Testes Periódicos

O presente Plano de Contingência será revisado anualmente pelo CTO ou, quando necessário, na ocorrência de alterações nos processos ou na estrutura adotados pela VELT Partners (seja por otimização, adequações, ou introdução de novas tecnologias) e estará sujeito à validação pela Diretora de Compliance e Gestão de Risco da VELT Partners.

Uma vez a cada 12 meses (ou em prazo inferior se assim for determinado), os Colaboradores que fazem parte do rol de Key Users da VELT Partners, nos termos deste Plano de Contingência, passarão por um teste simulando situações em que haja necessidade de acesso às Estações de Trabalho Virtuais, de modo a verificar a integridade, segurança e consistência dos bancos de dados, sistemas e arquivos e que estarão no exato estado imediatamente anterior ao acontecimento de um evento de desastre, bastando o seu acesso para que assegurada a continuidade dos negócios. O registro de participação nos testes será arquivado na sede da VELT Partners.

Todos os colaboradores têm acesso ao presente Plano de Contingência que fica disponível na plataforma do HUB da VELT Partners, linkada ainda ao Grupo do Teams dedicado aos assuntos de Compliance e Risco, e poderão acessá-lo, em sua versão mais atual, a qualquer tempo.