PLANO DE CONTINGENCIA

KIRON CAPITAL GESTÃO DE RECURSOS LTDA

Versão 1.0
Janeiro de 2019

Plano de Contingência

Plano de Contingência

1 INTRODUÇÃO

1.1 Objetivo

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

Os Eventos de Contingência são descritos detalhadamente nos manuais e políticas da KIRON, conforme aplicáveis, sendo considerados, por exemplo: a interrupção temporária na prestação de serviços de infraestrutura (energia elétrica, acesso a internet, telefonia), a ocorrência de impedimento no acesso à sede da KIRON (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 KIRON e dos Veículos de Investimento.

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

(i) A contínua execução de trades pelos Veículos de Investimento, com o correto atendimento às regras de compliance pertinentes;
(ii) A contínua execução das rotinas operacionais dos Veículos de Investimento e da gestora;
(iii) A comunicação regular entre Colaboradores, clientes e parceiros, seja mediante e-mail ou telefone;
(iv) O acesso ininterrupto aos sistemas, informações e arquivos licenciados ou de propriedade da KIRON.

2 MEDIDAS PREVENTIVAS

A KIRON 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 KIRON mediante prévia aprovação de um dos colaboradores. Ademais, a entrada de colaboradores no escritório é controlada por sistema de senhas pessoais, 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 de Infraestrutura**: a KIRON realiza anualmente, com o auxílio de terceiros prestadores de serviços, a reavaliação dos seus servidores, links de acesso a 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.

3 INFRAESTRUTURA DE TI E DISASTER RECOVERY

A infraestrutura da empresa (instalações, *hardware* e *software*) são todos de primeira linha e voltados a atender os investidores mais exigentes. Nesse sentido, a KIRON opera com uma política de redundância dupla, com servidores, storage e firewall duplicados internamente e também replicados em nuvem (Microsoft Azure e Amazon AWS). 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 substituído em tempo real, em uma estrutura de seamless integration que mantém todos os serviços em funcionamento.

Toda essa estrutura operacional visa garantir a manutenção do maior tempo de atividade possível ao escritório da KIRON. Ademais, a empresa conta com um acordo de serviços com um fornecedor de infraestrutura de TI e um fornecedor de segurança da informação, ambos disponíveis 24/7. Esses fornecedores conseguem trabalhar remotamente sobre quase a totalidade dos problemas e, caso necessário, estão comprometidos em mandar um técnico ao escritório para suporte.

O sistema de e-mail está localizado na nuvem (Microsoft 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 e gerador no prédio, que entra em serviço em média 8 segundos após uma falta de luz). Em adição, sempre há PCs de backup em caso de falha dos equipamentos existentes.

Vale destacar também, todas as permissões de rede/login/senha são sincronizadas online com o ambiente de *Private Cloud* tendo em vista a existência de um *domain controller* da rede. Ou seja, uma alteração de senha no ambiente de produção é replicada no ambiente de *Private Cloud* em questão de segundos, 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.

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 KIRON é protegido por firewall operando em redundância e com monitoramento 24/7, 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 KIRON, bem como redundâncias em nuvem, distribuídos entre Microsoft (Azure) e Amazon Web Services.
Arquivos	Localizados no escritório da empresa situado na Rua Tabapuã, com cópias digitalizadas disponíveis no servidor local em regime de espelhamento em tempo real entre dois servidores ("bridge") e no datacenter da Microsoft, em regime de back-up diário, com histórico e controle de versionamento.
E-mails	Armazenados e fluem através de uma solução em nuvem da Microsoft (Office365), com retenção dos últimos 5 anos.

PABX/ Telefonia	Disponível via Amazon Web Services e também no banco de dados do prestador de PABX (Option Telefonia), sendo que há uma programação prévia para que, uma vez ativado o sistema, este transfira todas as ligações feitas aos ramais da Empresa para os respectivos celulares pessoais dos colaboradores.
Desktops Virtuais	Disponíveis 4 Desktops Virtuais no datacenter do prestador de serviços de infraestrutura de TI da KIRON, 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 com Two Factor Authentication, 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.

4 PROCEDIMENTOS

4.1 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 – Sistemas Cobertos, e/ou em seus servidores e rede, o Comitê de Segurança da Informação, em parceria com os prestadores de serviço de TI, atuará 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 KIRON, os colaboradores devem se orientar para que o acesso seja feito remotamente e conforme o guia de acesso remoto via VPN.

Falha de Infraestrutura:
(a) Energia Elétrica: caso haja falha no fornecimento de energia, a KIRON conta com um nobreak com autonomia de 1 hora de bateria, além do gerador no prédio, que é inicializado automaticamente em até 8 segundos da ocorrência da queda de energia.

- Principais Ações e Responsáveis: Caso os back-ups de eletricidade elencados acima não funcionem ou sejam insuficientes, o Comitê de Segurança da Informação orientará os Key Users para que se desloquem até suas casas e deem continuidade operacional aos trabalhos via acesso aos Desktops Virtuais.

(b) Comunicações: a KIRON 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 dois *firewalls* operando simultaneamente, em redundância ("*bridge*"). Da mesma forma, os serviços de telefonia estão provisionados em núvem da Amazon Web Services, além de todos os ramais serem conectados por PABX, configurado por meio de uma VPN IP, permitindo assim o fornecimento de link de voz ininterrupto.

- Principais Ações e Responsáveis: Caberá ao Comitê de Segurança da Informação 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 KIRON, 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 KIRON, ficará a cargo do Comitê de Segurança da Informação e do Diretor de Compliance e Gestão de Riscos 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, através de qualquer computador, acessar os computadores virtuais que ficam disponíveis 24/7.

4.2 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 Comitê de Segurança da Informação, pelo Diretor 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 funções críticas da KIRON, com a maior brevidade possível;
(iii) comunicar aos demais colaboradores acerca do referido plano de ação e se necessário, convoca-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 problemas decorrentes do Evento de Contingência ou Desastre e restabelecidas, em sua integralidade, as funções e atividades da KIRON.

4.2.1 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 do Diretor de Compliance e Gestão de Risco e de um integrante do Comitê de Segurança da Informação.

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

4.3 Revisões Periódicas

O presente Plano de Contingência será revisado anualmente pelo Diretor de Compliance e Gestão de Risco, ou quando ocorrerem de alterações nos processos ou na estrutura adotados pela KIRON (seja por otimização, adequações, ou introdução de novas tecnologias), se necessário.

Todos os colaboradores receberão uma cópia do presente Plano de Contingência, em conjunto com o Manual de Compliance, Código de Ética e Política de Cibersegurança, além de poderem acessá-lo, em sua versão mais atual, a qualquer tempo, no website da empresa.