Canepa
Asset Brasil

PLANO DE CONTINUIDADE DOS NEGÓCIOS

Dezembro 2018

Versao atual: dezembro/2018
Versão anterior: junho/2016

Canepa
Asset Brasil

Versão atual: dezembro/2018
Versão anterior: junho/2016

1. INTRODUÇÃO

Este Plano de Continuidade de Negócios ("Plano") considera os procedimentos que deverão ser seguidos pela Canepa Asset Management – Cam Brasil Gestão de Recursos Ltda. ("**Canepa**") visando a continuidade de seus negócios nos casos de contingência. O Plano é estruturado de acordo com a análise dos riscos potencias de cada variável de infraestrutura (energia, telecomunicação, informática e sistemas internos).

2. INFRAESTRUTURA

O backup dos servidores, sistemas e chamadas telefônicas é realizado utilizando-se do arcabouço das melhores práticas em segurança da informação. Os meios de armazenamento atendem os 3 níveis de segurança (espelhamento entre servidores, nuvem e HD externo) e nunca são excluídos do site de recuperação de desastre (backup online), mesmo que sejam excluídos do site principal. Arquivos abertos (outlook e outros como bancos de dados) também são espelhados enquanto estão em uso.

A operacionalização será o quanto possível documentada para que um usuário experiente do software possa restaurar os dados. Além disso, será configurado para alertar automaticamente o administrador para o status de qualquer backup, sinalizando para o sucesso ou falha das cópias.

O backup online completo dos sistemas será realizado diariamente, ao fim do dia. O backup local em HD externo é realizado diariamente, atualizando os arquivos alterados de segunda à quinta e todos os arquivos na sexta-feira, mensalmente no último dia do mês e anualmente no último dia do ano. A exceção deste processo ocorre para os sistemas cujos dados e informações são armazenados pela própria empresa fornecedora (LOTE45), em seus servidores, os quais seguem regras próprias de segurança.

A retenção do backup em HD externo para os diários é de 4 (quatro) semanas, mensais de 12 (doze) meses e anuais de 5 (cinco) anos. A retenção dos dados na nuvem contempla sempre as últimas 10 (dez) alterações de cada arquivo

Mídias removíveis serão substituídas periodicamente com fins de preservação da mesma.

Além dos mecanismos convencionais para garantir a integridade das informações, como backup em servidores com hardware redundante, a **Canepa** replica diariamente todos os seus arquivos em servidor secundário, assim como realiza semanalmente a clonagem do sistema operacional para rápida recuperação.

A detecção automática de falhas em servidor de monitoramento (NAGIOS e ZABBIX) permite a prevenção de indisponibilidade em todos os hardware (servidores), software e links (Broadcast, Bloomberg, internet e site, por exemplo).

A **Canepa** conta com linhas de telefones digitais e 2 (dois) aparelhos de celular em caso de emergência. Além disso, todos os funcionários possuem celular que podem substituir a telefonia fixa.

Em caso de falha de fornecimento de energia, a **Canepa** possui nobreak para suporte por um tempo limitado para o funcionamento de seus servidores e estações de trabalho. A unidade de quebra de fornecimento de energia conta com capacidade de processamento ininterrupto das operações (unidades de UPS – Uninterruptiple Power Supply).

O serviço de e-mail da **Canepa** é fornecido pela Microsoft, com suporte 24/7, serviço de anti spam, com acesso remoto de todas as mensagens pelos colaboradores.

As informações do portfólio, além de estarem nos sistemas internos, constando com todos os processos de redundância acima informados, também são disponibilizados pelo administrador dos fundos, permitindo mais uma linha de contingência em caso de problemas na rede de arquivos da **Canepa**. As informações do passivo dos fundos de investimento sob gestão são monitoradas e armazenadas pelos administradores e distribuidores dos fundos.

A Canepa conta com notebooks de contingência preparados com todas as ferramentas necessárias (Broadcast, Lote45 e Microsoft Office, por exemplo).

3. PROCEDIMENTOS

Para que seja caracterizada uma situação de emergência, o impedimento à execução das atividades essenciais deve ser por tempo prolongado ou indeterminado. Considera-se tempo prolongado sempre que o tempo transcorrido desde a interrupção da atividade alcance 24 horas, a expectativa de tempo até a solução da interrupção seja superior a 24 horas, quando o tempo remanescente para a conclusão da atividade for insuficiente para sua execução no mesmo dia ou se a não execução imediata da atividade puder provocar prejuízos para os fundos sob gestão.

Caso a situação de emergência implique na inviabilidade de se utilizar o espaço físico do escritório, a **Canepa** pode funcionar em qualquer escritório da empresa Regus.

O CEO deverá entrar em contato com a Regus, efetuar a reserva e indicar os colaboradores que irão para o site de contingência. Adicionalmente, deverá notificar a empresa de suporte de tecnologia contratada.

Deverão ser encaminhadas para o local de contingência as pessoas responsáveis pelas funções de: boletagem e conferência das operações junto ao administrador, os principais gestores da carteira, o Diretor de Compliance e Riscos, além do CEO.

Se a impossibilidade de se utilizar o espaço físico da **Canepa** ocorrer quando os colaboradores estiverem no escritório, os colaboradores selecionados pelo CEO irão se dirigir diretamente ao escritório da Regus portando os notebooks de contingência da empresa. Caso a impossibilidade de utilizar o espaço ocorra quando os colaboradores não estiverem no escritório, eles serão notificados por meio eletrônico.

O Diretor de Compliance e Riscos ou o Diretor Administrativo serão os responsáveis por coordenar o responsável de TI no processo de recuperação dos arquivos, mediante utilização do backup diário realizado na nuvem.

4. TESTES DE CONTINGÊNCIA

Será planejada a realização de testes de contingências ao menos 1 (uma) vez a cada 12 (doze) meses com o objetivo de verificar se este Plano é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da instituição e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se o mesmo pode ser ativado tempestivamente.

O resultado de cada teste será registrado em relatório próprio obedecendo o disposto na regulamentação aplicável e as orientações das entidades responsáveis pela supervisão das atividades. Ademais, o referido relatório também servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento do presente Plano.