# MANUAL DE CONTROLES INTERNOS
# POLÍTICAS & NORMAS INTERNAS

---

## PLANO DE CONTINUIDADE DE NEGÓCIOS

## Princípios Gerais - Objetivo

O objetivo deste Plano de Continuidade de Negócios (PCN) é estabelecer responsabilidades, ações, e procedimentos para permitir a recuperação dos dados, comunicação, e ambiente de rede da empresa no evento de uma interrupção inesperada. O plano é estruturado para atender os seguintes objetivos:

**a)** Recuperar a estrutura da rede física da empresa dentro de parâmetros aceitáveis (especialmente de prazo) para o negócio e definido neste documento;

**b)** Recuperar os aplicativos e dados usados pela empresa dentro de parâmetros aceitáveis (especialmente de prazo) para o negócio e definido neste documento;

**c)** Recuperar a estrutura de comunicação da empresa dentro de parâmetros aceitáveis (especialmente de prazo) para o negócio e definido neste documento; e

**d)** Minimizar o impacto no negócio em termos de perdas monetária e interferência operacional.

**Para atingir esse objetivo, este documento foi estruturado em 3 partes, quais sejam:**

1) Identificação do responsável pelo PCN e suas responsabilidades
2) Planejamento de infraestrutura e procedimentos para viabilizar o PCN
3) Procedimentos de recuperação pós-interrupção no caso de um evento inesperado

## Identificação dos Responsáveis pelo Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios está sob a responsabilidade do Comitê Executivo da AGBI. Entre suas responsabilidades estão:

**a)** Promover o planejamento da estrutura de TI e de comunicações para permitir um rápido reestabelecimento do negócio em caso de interrupções ou desastres

**b)** Contato com prestadores de serviço para recuperar dados e infraestrutura;

**c)** Liderança junto à equipe da AGBI Ativos Reais Ltda. para atendimento aos procedimentos identificados nessa política.

## Planejamento de infraestrutura e procedimentos para viabilizar o PCN

A eficácia do Plano de Continuidade de negócios da AGBI depende não somente das diretrizes traçadas nesse plano, como também do respeito às políticas internas da empresa, em particular a Política de *Home Office*. Visando definir um ambiente seguro e facilmente recuperável, a AGBI colocou em vigor uma política de segurança de dados, além de uma política de uso de recursos de computação e comunicação, que estabelecem os procedimentos a serem seguidos por seus colaboradores em relação às informações da empresa e sua infraestrutura, além de definir as bases necessárias para a continuidade dos negócios em caso de interrupções não programadas ou desastres. Os procedimentos servem seu propósito tanto para o trabalho remoto (*home office*) quanto presencial e, consequentemente, facilitam a transição de um para o outro sem prejuízo aos dados, segurança de informação e produtividade da gestora.

Além disso, para viabilizar um PCN que permita à AGBI proteger suas informações de negócio e reestabelecer as condições de trabalho de forma eficiente e rápida após a ocorrência de um evento de interrupção parcial ou permanente, foi realizado um planejamento da infraestrutura e serviços de TI de forma a permitir a recuperação de dados e comunicação em um curto espaço de tempo, seja no escritório da AGBI, seja em um site remoto.

Foi adotada uma estratégia de Contingência *Cold-site* a partir da qual a empresa poderia se relocar para um ambiente com recursos mínimos de infraestrutura e telecomunicações e as pessoas operarem a partir de notebooks disponibilizados pela empresa. Também há uma Política de *Home Office* que já prevê procedimentos e requisitos mínimos para o desempenho das funções da empresa de forma remota sem prejuízos. Ainda, foi estabelecido, no âmbito da Política de *Home Office*, uma série de procedimentos operacionais padrão (POP) para melhora para qualidade da comunicação virtual, contemplando desde etiqueta em ligações de áudio e vídeo até melhores práticas no envio de documentos e arquivos.

**Servidor de Arquivos:** temos nossa base de dados armazenada localmente em dois servidores espelhados. O back-up local é feito diariamente, podendo ser recuperado em poucas horas (um arquivo pode ser recuperado em poucos minutos) pelo administrador do sistema, sendo que o backup remoto pode ser recuperado em um prazo máximo de 24 horas após a solicitação do administrador do sistema. Desta forma, caso haja desastre em nossas instalações estamos totalmente aptos a continuar as atividades em qualquer outra localização imediatamente. A armazenagem remota elimina problemas associados a eventos naturais que poderiam afetar sites numa mesma localidade.

**Servidor de E-mail:** a AGBI optou por contratar um servidor de e-mail na nuvem de classe empresarial fornecido pela Microsoft através de seu produto Office 365 pacotes E3. Esse serviço além de contar com uma alta disponibilidade com garantia de 99.9% de tempo de serviço, se

beneficia da infraestrutura de datacenters da Microsoft, com redundância de servidores e políticas de *compliance* e segurança de classe empresarial. Por ser baseado em um servidor na nuvem, em caso de impossibilidade de uso do escritório da AGBI, o serviço poderia ser facilmente reestabelecido em um site remoto através de webmail ou da configuração de novos computadores para acesso ao servidor. Ainda, foram adotados diversos procedimentos de armazenamento de redundância na rede utilizando o programa Microsoft OneDrive, de armazenamento de arquivos na nuvem, para facilitar a operação remota dos colaboradores da AGBI.

**Comunicação:** utilizamos serviços de voz e dados de nível corporativo da Vivo, além de contar com redundância do serviço de dados com e linhas de celular corporativas da VIVO para a equipe.

Dado o perfil dos fundos geridos (poucos ativos, investimentos em empresas fechadas, normalmente 1-3 investimentos por ano por fundo, etc.), não foi identificado um alto risco de falta de continuidade para o negócio. O ponto mais importante no caso de uma eventual interrupção seria restaurar as bases de dados (contendo as informações de análise e gestão dos investimentos do pipeline e dos ativos investidos dos fundos, relatórios e controles gerenciais etc.) e a infraestrutura básica para operação do dia a dia de um fundo voltado para *private equity* (computadores/notebooks, rede básica de telefonia e infraestrutura básica de acesso aos dados armazenados nos servidores e website).

## Infraestrutura Atual da AGBI Ativos Reais Ltda.

**a)** 7 computadores desktop HP e 2 notebooks;

**b)** No break para contingenciamento de energia para os computadores locais;

**c)** Infraestrutura de rede ligada a link de 100 mega da Vivo;

**d)** Rede de telefonia da Telefônica com 10 linhas individuais e 20 ramais;

**e)** Servidores remotos com capacidade de armazenamento virtualmente ilimitada acrescida conforme nossas necessidades de forma incremental. Estes servidores realizam o backup dos dados dos usuários individuais diariamente e estes dados podem ser recuperados a partir de qualquer computador acessando a internet mediante login e senha devidamente validados;

**f)** Sistema de e-mail da Microsoft, contendo infraestrutura de firewalls e antivírus. Além disto, possuímos sistemas anti-virus em nossos computadores individuais;

**g)** Pacotes Windows e Microsoft Office nos computadores da empresa, incluindo Microsoft OneDrive.

## Procedimentos de Recuperação da Infraestrutura e Serviços da Empresa

A AGBI possui um plano de contingência e continuidade do negócio simples e eficaz, para garantir que em caso de qualquer tipo de incidente que impossibilite a entrada, deslocamento ao escritório da empresa ou que implique na evacuação do local, todos os colaboradores possam dar continuidade a suas atividades, seguindo o fluxo a seguir:

**1.** Caso haja qualquer tipo de evento que impossibilite o acesso ao escritório, foi instituído que a Sra. Josefa e Sra. Dilaine, primeiras colaboradoras a chegarem/tentarem acessar o escritório, entram em contato com o Sr. Gustavo. Ou caso haja necessidade de evacuação do escritório, os sócios Gustavo e Luciano levarão os seus notebooks e a sra. Dilaine e o sr. Diogo levarão os outros dois notebooks existentes na empresa para o ambiente de contingência, se a situação permitir seu o transporte, de forma que todos consigam trabalhar rapidamente e seguir da melhor forma executando suas atividades;

**2.** Ao receber o alerta de incidente ou enfrentar a situação de evacuação, o Sr. Gustavo irá informar (Ligação/WhatsApp) os colaboradores que não estiverem no escritório sobre a situação e acionamento do plano de contingência;

**3.** Cada colaborador será comunicado sobre o momento em que deverá se deslocar ao ambiente de contingência e se o deslocamento não for imediato, o colaborador deverá retornar/permanecer em sua residência e trabalhar em *home office*;

**4.** A equipe de TI terceira é acionada juntamente com a equipe dos colaboradores da empresa no item 2, e adotará os procedimentos abaixo:

**4.2** Configuração de resposta automática dos e-mails, para todos os colaboradores com a seguinte mensagem “No momento a equipe da AGBI está impossibilitada de ter acesso a algumas informações e pode ter algum problema em receber essa mensagem via e-mail e receber chamadas em seus telefones no escritório. Por gentileza entrar em contato com o sócio Sr. Gustavo Fonseca pelo número: (11) 99246-0733”;

**4.3** Deslocamento ao local estabelecido como ambiente de contingência, para auxílio no acesso as informações dos arquivos de backup existentes, em um disco externo físico

que fica em posse do Sr. Gustavo e que conterá o backup de, no mínimo, a última semana de atividade da empresa;

**4.4** Independente do incidente inviabilizar o acesso ao escritório por tempo indeterminado, a equipe de T.I. providenciara um servidor que será disponibilizado no ambiente de contingência, para o retorno do backup retorno realizado também em nuvem utilizando o serviço do Microsoft Azure Backup, o qual temos a retenção por 12 meses, com backups completos diários, por se tratar de uma solução integrada ao sistema operacional do Servidor, este backup só é utilizado em situações extremas.

**5.** Quando os colaboradores estiverem no ambiente de contingência serão disponibilizados notebooks ou recursos de processamento para pessoas chave de modo a restaurar o quanto antes o fluxo de análises, relatórios e informações dentro e fora da empresa, se não houver disponibilidade de notebooks para todos trabalharem ou caso o transporte dos notebooks existentes no escritório não tenha sido possível, a aquisição de novos notebooks pode ser viabilizada em 24-48 horas;

**6.** Utilização dos telefones celulares corporativos até o reestabelecimento das linhas fixas ou divulgação de novos números de contato de contingência;

**7.** Retomada das comunicações por e-mail através da configuração do servidor de e-mail nos novos computadores ou acesso via webmail. Por ser um serviço remoto, o acesso ao e-mail através dos smartfones corporativos não deve ser prejudicado em caso de problemas que afetem o escritório da AGBI;

**8.** Ativação do link secundário de internet em caso de falha de serviço no link primário da Vivo;

**9.** Assim que o acesso ao escritório for reestabelecido, a equipe de T.I. fará a cópia dos arquivos alterados na execução do plano de contingência, e os sincronizará dentro do servidor da AGBI, todas as verificações necessárias para garantir a integridade dos dados serão verificados, o comunicado previamente configurado no e-mail de cada colaborador será desativado e a AGBI entra em modo operação normal.