POLÍTICA DE CONTINUIDADE DOS NEGÓCIOS

SDI GESTÃO E CONSULTORIA DE INVESTIMENTOS LTDA.

I. Introdução

1.1. A presente Política de Continuidade dos Negócios ("Política") da SDI GESTÃO E CONSULTORIA DE INVESTIMENTOS LTDA. ("SDI") tem por objetivo definir os procedimentos que deverão ser seguidos, em relação a contingência, para que a SDI evite risco de descontinuidade operacional em situações de falta de acesso ao escritório sede.

1.2. A presente política visa detalhar o plano de continuidade dos negócios em momentos de contingência ou desastres, definindo assim as diretrizes, responsabilidades e recomendações adotadas pela SDI em suas atividades, em conformidade com a exigência da resolução nº 2.892 de 26 de maio de 1999, emitida pelo Banco Central do Brasil ("Resolução Bacen nº 2.892"), que dispõe sobre a implementação de estrutura de continuidade dos negócios em momentos de contingência ou desastres.

II. Introdução

2.1. Para garantir a continuidade dos negócios em quaisquer eventos de contingência ou desastres que possam impactar os serviços prestados, a SDI conta com uma área com o mandato de estabelecer critérios e analisar os eventos com independência para acionar todas as diretrizes descrita neste documento.

2.2. A Área de Risco e Compliance terá as seguintes atribuições:

(i) Monitorar a operação e os respectivos eventos de contingência e desastre;

(ii) Garantir com a área de Tecnologia da Informação ("TI") o funcionamento da estrutura operacional de contingência e desastre;

(iii) Aprovar anualmente orçamento e novas diretrizes da política.

III. Estrutura de Contingência Operacional

3.1. Backup de Dados. Diariamente, todos os arquivos localizados na rede da SDI são enviados para o serviço de backup on-line (backup na nuvem) chamado DROPBOX Bussiness, de maneira automática.

3.1.1. O serviço de backup on-line é acessado somente pelo TI através de um painel via navegador (browser) com usuário e senha.

3.1.2. O serviço de backup on-line permite a recuperação de qualquer versão anterior dos arquivos a qualquer momento.

3.1.3. Caso um grande volume de dados seja apagado, imediatamente, é enviado um e-mail de alerta ao TI da SDI e os arquivos podem ser recuperados durante um prazo de 30 dias.

3.1.4. Todo o procedimento operacional acima descrito é de responsabilidade do TI da SDI.

3.1.5. Os dados permanecem no servidor da SDI e são replicados na nuvem automaticamente.

3.1.6. O procedimento operacional acima descrito será testado em periodicidade máxima trimestral. Faz parte do teste a recuperação de arquivos do ano corrente e de anos anteriores. A responsabilidade pelo procedimento de avaliação é da Área de Risco e Compliance da SDI.

3.1.7. Estão contemplados neste procedimento todos os arquivos e e-mails arquivados na rede da SDI. Cabe ressaltar que não estão contemplados neste procedimento os arquivos localizados nos discos rígidos dos equipamentos utilizados pelos Colaboradores.

3.2. Contingenciamento do fornecimento de energia. A SDI possui na sua infraestrutura uma redundância de energia elétrica em casos de falta da distribuição pela empresa contratada. O processo de contingenciamento é feito em 2 (duas) etapas, sendo elas:

(i) Entrada automática de energia fornecida pelos 10 nobreaks existentes que totalizam 25 KvA (as baterias suportam 2 horas do escritório em plena função);

(ii) Entrada automática do Gerador a diesel de 500 KvA, após 15 a 20 segundos da queda de energia. O gerador da SDI tem autonomia no seu tanque 900 litros de combustível reabastecível para suportar 14 horas de funcionamento total da SDI.

3.3. Contingenciamento de links de internet e telefonia. A SDI possui redundância de links de internet e de telefonia em sua infraestrutura operacional:

(i) **Links de Internet:** Há um link primário corporativo de Internet de 70 MB com 1 IP fixo da TIM e outro link de 25 MB da Vivo com um único IP fixo.

(ii) **Telefonia:** A Central telefônica primária com até 192 ramais na AVAYA IPO500 com telefonia híbrida (IP, digital e analógica) Telecom e os mesmos respectivos ramais contingenciados na Vivo.

3.4. Acesso Remoto: No caso de impossibilidade de acessar o escritório, os Colaboradores poderão acessar os servidores em Nuvem com senhas próprias e dar continuidade aos negócios de qualquer local, visto que a SDI atua exclusivamente com fundos estruturados (considerando sua essência e também o fato de não apresentarem quota diária). A SDI possui estrutura de e-mail corporativo via provedor, permitindo acesso online via web por todos os Colaboradores e em qualquer lugar que possua internet.

IV. Plano de Continuidade de Negócios em Desastres

4.1. O plano de contingência operacional visa proporcionar a manutenção dos serviços da SDI nas seguintes áreas: (i) Novos Negócios; (ii) Gestão de Ativos, (iii) Área de Risco e Compliance e (iv) Consultoria Financeira.

4.2. Os processos para declarar contingência estão descritos abaixo:

(i) A Área de Risco e Compliance monitora e identifica o evento de contingência ou desastre;

(ii) A Área de Risco e Compliance avalia o evento com a diretoria executiva e declara contingência;

(iii) A Área de Risco e Compliance comunica o TI para subir a contingência, liberar as VPNs e redirecionar os ramais;

(iv) A Área de Risco e Compliance faz a comunicação aos responsáveis de cada área para se locomover para locais onde possam dar continuidade aos negócios da SDI.

4.3. Anualmente irá haver 1 (um) teste de contingência para homologar a estrutura operacional.

V. Documentação e Armazenamento

5.1. Toda informação referente ao gerenciamento da Área de Risco e Compliance deve ser devidamente documentada e armazenada pelo prazo mínimo de 05 (cinco) anos.

5.2. A documentação e armazenamento devem garantir a exatidão, veracidade e integridade da informação e suas respectivas evidências. Assim como acesso somente as pessoas devidamente autorizadas pela Área de Risco e Compliance da SDI.

VI. Dúvidas

6.1. Quaisquer dúvidas relacionadas com a presente política devem ser esclarecidas com a Área de Risco e Compliance da SDI.