POLÍTICA DE CONTINUIDADE DOS NEGÓCIOS

HERMON CAPITAL GESTÃO DE RECURSOS LTDA.

I. Introdução

1.1. A presente Política de Continuidade dos Negócios ("Política") da HERMON CAPITAL GESTÃO DE RECURSOS LTDA. ("Hermon") tem por objetivo definir os procedimentos que deverão ser seguidos, em relação a contingências, para que a Hermon 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 Hermon em suas atividades.

II. Área de Risco e Compliance

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

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

(i) Monitorar as operações da Hermon e os respectivos eventos de contingência e/ou desastre;

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

(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 Hermon são enviados para o serviço de backup on-line (backup na nuvem) chamado Cloudberry Backup - MSP360, uma das líderes mundiais de sistemas de back-up e armazenamento para empresas, 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, ressalvado o prazo de armazenagem de 5 (cinco) anos por arquivo.

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

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

3.1.5. Os dados permanecem no servidor da Hermon 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 Hermon.

3.1.7. Estão contemplados neste procedimento todos os arquivos e e-mails arquivados na rede da Hermon. 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 Hermon possui na sua infraestrutura uma redundância de energia elétrica em casos de falta da distribuição pela empresa contratada, conforme detalhado abaixo:

(i) Entrada automática de energia fornecida pelos 3 (três) nobreaks existentes, sendo cada um com 4,2 KvA, cujas baterias suportam 3 (três) horas do escritório em plena função.

3.3. Contingenciamento de links de internet e telefonia. A Hermon 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 600 MB (seiscentos megabytes) da operadora ALGAR Telecom com IP dinâmico e com DDNS implantado e outro link de 300 MB (trezentos megabytes) da operadora VIVO com IP dinâmico e DDNS implantado. Esses links são gerenciados por equipamento UDM Pro da Ubiquiti Networks com Failover automático e gerenciamento completo.

(ii) **Telefonia:** Há uma central telefônica primária com Link E1 digital com 30 (trinta) juntores e capacidade para 96 (noventa e seis) ramais analógicos e 4 (quatro) IP atualmente, podendo ser expandida para até 160 (cento e sessenta) ramais analógicos e para 120 (cento e vinte) ramais IP. Link E1 é fornecido pela operadora ALGAR.

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. A Hermon 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 Hermon 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; e

(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 Hermon.

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 o armazenamento devem garantir a exatidão, veracidade e integridade da informação e suas respectivas evidências. Assim como acesso somente às pessoas devidamente autorizadas pela Área de Risco e Compliance da Hermon.

VI. Dúvidas

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