POLÍTICA DE CONTINGÊNCIA

DA

IBRRA GESTÃO DE RECURSOS LTDA.

Sumário

1. Objetivo

A Política de Contingência tem como objetivo definir o Plano de Contingência e Recuperação de Desastres ("Plano de Contingência") a ser seguido pela IBBRA Gestão de Recursos LTDA. ("IBBRA Gestão"), de modo a impedir a descontinuidade operacional da IBBRA Gestão, determinando os procedimentos que deverão ser seguidos visando proteger os interesses dos Investidores e a continuidade das atividades.

Além disso, a IBBRA Gestão possui uma Política Segurança da Informação que estabelece regras, processos e diretrizes a serem observadas por todos os colaboradores da IBBRA Gestão que, em virtude da execução de seu trabalho tenham acesso a informações relevantes relativas a IBBRA Gestão, com a finalidade de assegurar a segurança das informações que estiverem sob sua posse e guarda, inclusive aquelas armazenadas ou disponibilizadas nos equipamentos cedidos pela IBBRA Gestão para exercício de suas funções, sendo de responsabilidade do Colaborador a garantia de sua confidencialidade.

2. Evento/ Ameaças Previstos

O Plano de Contingência da IBBRA Gestão traz como principais eventos/ameaças aos negócios da IBBRA Gestão:

- Baixa conectividade ou perda de conectividade com a internet;
- Invasão sistêmica que prejudique dados internos;
- Falha nas linhas telefônicas;
- Inacessibilidade temporária do escritório;
- Inacessibilidade permanente do escritório;
- Inacessibilidade dos Diretores responsáveis por tomada de decisão por mais de 24 horas; e
- Qualquer outra situação que ameace o ambiente da IBBRA Gestão, mesmo que não descrita acima.

3. Procedimento Interno (Pessoas Chave)

Em caso de efetiva necessidade de implantação do Plano de Contingência, deverão ser encaminhadas para o local ou área de contingência as "Pessoas Chave", que avaliarão o evento ou ameaça e determinarão os deveres e responsabilidades dos demais colaboradores. Tais "Pessoas Chave" são previamente identificadas desta forma e informadas de suas atribuições pelo Diretor de *Compliance* e Risco. As funções prioritárias de "trigger" do Uso do Local Alternativo; Contato com colaboradores; Contato com

Investidores e Contra-partes; Confiabilidade dos Dados Armazenados / Recuperados são atribuídas aos diretores da IBBRA Gestão e ao Diretor de *Compliance* e Risco.

4. Proteção e recuperação de dados e documentos

Todos os arquivos armazenados nos computadores utilizados pelos colaboradores da IBBRA Gestão são objeto de *backup* periódico. Este *backup* é feito em disco rígido (HD) e ao menos uma cópia é mantida fora do ambiente da IBBRA Gestão. Além disso, a IBBRA Gestão possui também um servidor de *firewall* para controlar o tráfego de informação digital, e que também cuida da VPN, que permite o acesso seguro dos usuários de locais remoto. A Direção de Compliance supervisionará o acesso às informações contidas nos backups e somente se utilizará dessas informações para fins internos ou nos termos previstos na lei.

Em detalhes, hoje contamos com 01 servidor virtualizado com proxmox, onde se encontra o local de nossos arquivos, temos todo o controle de acesso de senha, grupos de permissões, registro de logs e principalmente backups automáticos e diários de nossos arquivos em um local separado dentro do nosso servidor. Esse servidor permite acesso remoto, flexibilizando o trabalho em home office, mantendo toda a segurança que já é feita e presencialmente, mantendo todos requisitos de segurança de acesso aos arquivos. Também contamos com uma estrutura sólida de rede e firewall para controle e segurança.

Além disso, fazemos backup físico em HDs e também em cloud, utilizamos o sistema de Buckets da AWS Amazon S3 fora do servidor, para eventuais falhas ou perda de arquivos.

5. Comunicação Pública

A informação é um bem essencial para a operação das atividades da IBBRA Gestão e assim como seus ativos, deve ser adequadamente gerenciada e protegida por todos os colaboradores. Independentemente de sua forma ou divulgação, toda informação sob posse ou guarda dos colaboradores da IBBRA Gestão deverá ser tratada com os mais altos níveis de diligência, ética e profissionalismo. Toda informação deverá ser utilizada unicamente e exclusivamente para a finalidade para a qual foi autorizada.

Todas as declarações envolvendo a IBBRA Gestão ou qualquer assunto relacionado a ela, devem ser aprovadas pelo Diretor de *Compliance* e Risco que, a qualquer tempo e sem aviso prévio, poderá verificar o conteúdo das ligações telefônicas gravadas, dos arquivos disponíveis no diretório interno e dos e-mails enviados e recebidos, sem que isto configure quebra de sigilo, para fins de monitoramento do fiel cumprimento das normas de Compliance e das normativas legais pertinentes às atividades da IBBRA Gestão.

Caso ocorra um evento ou ameaça cujo resultado seja a inacessibilidade temporária ou permanente do escritório, a área de Compliance é responsável por elaborar comunicado formal aos Investidores, terceiros

contratados e ao mercado em geral. Na impossibilidade de atuação da área de Compliance, apenas os Diretores Executivos da IBBRA Gestão têm a autonomia para divulgar informações em nome da IBBRA Gestão, inclusive através da mídia e redes sociais, sempre respeitando o Código de Ética e demais políticas. Sendo absolutamente vedado aos demais colaboradores a comunicação pública sobre o ocorrido.

6. Avaliação e teste periódicos

O Plano de Contingência é avaliado e testado periodicamente em virtude das mudanças naturais ocorridas IBBRA Gestão, tais como entrada e saída de colaboradores, troca de sistemas, mudança de estratégia de proteção e etc. A execução deste teste é de responsabilidade da área de Compliance.

Infraestrutura

• Estações de Trabalho 1 – D. Gestão
1. Processador INTEL(R) CORE(TM) i5-8265U
2. 8GB DDR4 2400MHz
3. HD SATA 1000GB
4. Windows 10 HOME

• Estação de trabalho 2 – A. Gestão
1. Processador INTEL(R) CORE(TM) i5-8265U
2. 8GB DDR4 2400MHz
3. HD SATA 1000GB
4. Windows 10 HOME

• Estação de trabalho 3 – D. Compliance
1. Processador INTEL(R) CORE(TM) i5-8265U
2. 8GB DDR4 2400MHz
3. HD SATA 1000GB
4. Windows 10 PROFESSIONAL

• Estação de trabalho 4 – A. Compliance
1. Processador NTEL(R) CORE(TM) i3-5005U
2. 4GB DDR3 1600MHz
3 SSD SATA 240G
4. Windows 10 HOME

• Estação de trabalho 5 – A. Risco
1. Processador INTEL(R) CORE(TM) i3-8130U
2. 12GB DDR4 2400MHz
3. SSD SATA 240GB
4. Windows 10 HOME

II - Estação Firewall

1. Processador Intel Xeon 4-Core (3.0GHz)
2. 8GB DDR4 2133MHz
3. 01 HD SATA 1TB – 7.2k RPM
4. 01 HD SATA 2TB – 7.2K RPM
5. Proxmox VE 6.1-3
6. Pfsense 2.4.5

III – Servidor

1. Processador Intel Xeon 4-Core (3.0GHz)
2. 8GB DDR4 2133MHz
3. 01 HD SATA 1TB – 7.2k RPM
4. 01 HD SATA 2TB – 7.2K RPM
5. Proxmox VE 6.1-3

IV – Hardware

1. 01 linhas de telefone
2. 01 impressoras
3. 01 scanner/fax
4. 01 roteador wireless com criptografia
5. 01 No-Breaks

V - Software Básico

1. Anti-Virus WIDOWS DEFENDER MICROSOFT