POLÍTICA DE CONTINUIDADE DOS NEGÓCIOS

EVERGREEN INVESTMENT ADVISORS GESTORA DE RECURSOS LTDA.

I. Introdução

1.1. A presente Política de Continuidade dos Negócios ("Política") da EVERGREEN INVESTMENT ADVISORS GESTORA DE RECURSOS LTDA. ("EIA") tem por objetivo definir os procedimentos que deverão ser seguidos, em relação a contingências, para que a EIA 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 EIA em suas atividades. O escritório da EIA é supervisionado pela sua controladora, localizada em Chicago, assim como toda a logística do serviço de back-up, os quais obedecem aos mais altos padrões de segurança e de tecnologia da informação.

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 EIA 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 EIA e os respectivos eventos de contingência e/ou desastre;

(ii) Acionar a equipe de gerenciamento de crises, que é composta pelos (a) diretores Juliana Tagliati, Fernando Hamaoui, pelo (b) sócio Thomas Conway e pelo (c) time de Tecnologia da Informação ("TI"), formado pelos profissionais Kory Chan e Nick Matese ("Equipe de Gerenciamento de Crises").

(iii) Garantir com a área de TI o funcionamento da estrutura operacional de contingência e desastre; e

(iv) Aprovar anualmente orçamento e novas diretrizes da Política.

III. Estrutura de Contingência Operacional

3.1. Back-up de Dados. A EIA faz back-up de todos os registros eletrônicos do servidor estabelecido fisicamente no Brasil a cada 4 (quatro) horas, o qual ocorre remotamente via *data center* do escritório de sua controladora, em Chicago, através do serviço de back-up on-line chamado Veeam, líder mundial de sistemas de back-up e armazenamento para empresas, de maneira automática. Esses backups são armazenados em um servidor de backup imutável Exagrid, que possui exclusões de bloqueio de tempo de ransomware.

3.1.1. O serviço de back-up é acessado somente pelo TI através do aplicativo Veeam com usuário e senha.

3.1.2. O serviço de back-up 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, o sistema Netwrix Auditor notificará a equipe de TI da EIA para que a respectiva recuperação seja feita rapidamente através da utilização dos sistemas Veeam e Microsoft Shadow Copies, os quais possuem diversas camadas de recuperação.

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

3.1.5. Os dados permanecem no servidor da EIA.

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 EIA.

3.1.7. Estão contemplados neste procedimento todos os arquivos e e-mails arquivados na rede da EIA. 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 EIA 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 por um sistema APC UPS com 1 (um) nobreak existente, com 3000 kvA, cujas baterias suportam, no mínimo, 120 (cento e vinte) minutos do escritório em plena função.

3.3. Contingenciamento de links de internet e telefonia. A EIA possui links de internet e de telefonia em sua infraestrutura operacional, conforme detalhado abaixo:

(i) Links de Internet: Há um link primário corporativo de Internet de 100 MB da operadora Vivo com IP estatístico da própria empresa Vivo.

(ii) Telefonia: SIP fornecida pela Neo Telecom; Móvel fornecida pela Claro.

3.4. Acesso Remoto: No caso de impossibilidade de acessar o escritório, os Colaboradores poderão acessar os servidores da empresa com senhas próprias e dar continuidade aos negócios de qualquer local. A EIA possui estrutura de e-mail corporativo, permitindo acesso online via web por todos os Colaboradores e em qualquer lugar que possua internet, acesso este feito através de senha individual e utilizando a segurança e aprovação via VPN.

IV. Plano de Continuidade de Negócios em Desastres

4.1. O plano de contingência operacional visa responder a um desastre ou interrupção significativa dos negócios, proporcionando a manutenção dos serviços da EIA nas seguintes áreas: (i) Novos Negócios; (ii) Gestão de Ativos; (iii) Área de Risco e Compliance; e (iv) Administração Fiduciária. Assim, tal plano engloba todas as áreas operacionais da EIA, com o fim de recuperar e retomar rapidamente as operações, protegendo todos os registros da EIA.

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, com o apoio da Equipe de Gerenciamento de Crises, avalia o evento com a diretoria executiva e declara contingência;

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

(iv) A Área de Risco e Compliance, com o apoio da Equipe de Gerenciamento de Crises, faz a comunicação aos responsáveis de cada área para se locomover para locais onde possam dar continuidade aos negócios da EIA.

4.3. Anualmente haverá 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 EIA.

5.3. A EIA mantém seus principais livros e registros em papel e seus arquivos eletrônicos na cidade de São Paulo, sendo o Diretor de Compliance e Risco a pessoa responsável pela manutenção desses livros e registros, de forma que a EIA faz o back-up de seus arquivos eletrônicos diariamente em data center e mantém uma cópia em Chicago, Illinois, EUA.

5.4. Controle de Versões:

Data	Versão	Resumo das Alterações	Autor / Revisor
20/10/2023	1	N/A	Jacques Abi Ghosn / Fernando Hamaoui
02/10/2025	2	• Alteração da Denominação Social da Gestora/Administradora	Jacques Abi Ghosn

VI. Dúvidas

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

São Paulo, 02 de outubro de 2025.