PLANO DE CONTIGÊNCIA E CONTINUIDADE DOS NEGÓCIOS

Garín Investimentos LTDA

São Paulo – Fevereiro de 2019

Introdução

1. O presente Plano de Contingência e Continuidade de Negócios da **Garín Investimentos LTDA**. (o "**Plano de Contingência**" e a "**Sociedade**" ou **Garín**", respectivamente) tem como objetivo definir os procedimentos a serem seguidos no caso de contingência, de modo a impedir a descontinuidade operacional da Sociedade por problemas técnicos.

2. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da **Garín** sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre. O Diretor de Compliance é o responsável pela implementação do presente Plano de Contingência.

3. O Plano de Contingência prevê ações que durem até o retorno à situação normal de funcionamento da Sociedade dentro do contexto de seu negócio.

4. O Plano de Contingência da **Garín** identifica duas variáveis para o funcionamento adequado da empresa: (i) infraestrutura; e (ii) processos.

5. A infraestrutura engloba todas as variáveis utilizadas para realização dos processos, em particular: (i) energia; (ii) telecomunicações; (iii) informática; e (iv) sistemas internos. Para cada um dos itens que compõem a infraestrutura existe uma ação a ser tomada.

6. Já os processos são as atividades realizadas para operar os negócios da **Garín**. Os processos dependem da infraestrutura toda ou de parte da estrutura em funcionamento. Somente com os processos em andamento pode-se definir que o plano de ação foi bem executado.

Estrutura Operacional

7. A Sociedade tem como objeto a administração e gestão de recursos de terceiros, de modo que precisa contar com uma estrutura operacional desenvolvida e preparada para eventuais emergências. O suporte para essa estrutura operacional é um corpo funcional capacitado com áreas de apoio.

Análise de Risco

8. Com o objetivo de avaliar as medidas a serem tomadas em cada situação, serão analisados os cenários de risco e o potencial impacto nas operações da Sociedade, considerando sempre a probabilidade e a gravidade de ocorrência.

9. Dessa forma, considerando o impacto que pode ser causado para a **Garín** e seus clientes, é possível classificar os riscos em três categorias:

   Aceitável – quando a probabilidade de ocorrência e gravidade são baixos. Não é necessário tomar nenhuma medida.

   Tolerável – quando a probabilidade de ocorrência e gravidade são médios ou apenas um desses critérios é classificado como baixo ou grave. Nesta hipótese a Sociedade

está preparada para suportar o risco e continuar com as atividades, sem necessidade de acionar o Plano de Contingência.

Intolerável – quando a probabilidade de ocorrência e gravidade são altos. Deve ser aplicado o Plano de Contingência até que o risco seja controlado e as atividades possam voltar a normalidade.

Eventos de Risco

10. Para avaliação dos eventos possíveis causadores de situação de risco, leva-se em consideração, o patrimônio dos clientes, as informações confidenciais e privilegiadas, os Colaboradores, as instalações físicas, equipamentos de comunicação e informática.

Inacessibilidade ou restrição às instalações físicas com danos aos equipamentos

Hipótese de ocorrência: (i) eventos naturais; (ii) acidentes de grande natureza no entorno da sede social da **Garín**; e (iii) desastres internos

Probabilidade: Média

Gravidade: Baixa

Avaliação de Risco: Tolerável

Colaboradores

Hipótese de ocorrência: falecimento dos principais Colaboradores da Sociedade

Probabilidade: Baixa

Gravidade: Alta

Avaliação de Risco: Tolerável

Falhas no sistema de Segurança Cibernética e da Informação

Hipótese de ocorrência: vazamento de dados ou informações confidenciais e privilegiadas, invasão dos sistemas da Sociedade e aparelhos de informática ou de comunicação

Probabilidade: Baixa

Gravidade: Alta

Avaliação de Risco: Tolerável

Serviços de telefonia, internet e energia

Hipótese de ocorrência: interrupção temporária dos serviços terceirizados de telefonia, internet e energia elétrica

Probabilidade: Média

Gravidade: Baixa

Avaliação de Risco: Tolerável

Política e procedimentos para *backup*

11. Diariamente, todos os arquivos localizados na rede de arquivos da Sociedade são copiados, de maneira automática, para um Hard Drive do servidor. Os meios de armazenamento são Hard Drive no servidor, e Nuvem serviço Microsoft Cloud.

12. O *backup* se dará da seguinte forma: (i) para a garantia do *backup* das informações da **Garín**, estas devem ser armazenadas nos servidores da rede corporativa; (ii) não haverá garantia de *back-up* para arquivos armazenados nas estações de trabalho (desktops ou notebooks); (iii) o *backup* de dados nos servidores da rede corporativa é realizado de forma automatizada e periódico (1 vezes por dia às 22 horas), de acordo com os procedimentos de *backup* e *restore* definidos profissionais da área de tecnologia contratados pela Sociedade; (iv) o *backup* é armazenado no Hard Drive do servidor de *Backup* local; (v) o *restore* de dados deve ser solicitado aos profissionais contratados para a execução dos serviços de informática e será realizado de acordo com os procedimentos específicos do mesmo. A cópia de segurança deverá ser armazenada fora da Sociedade, sendo auditada periodicamente; e (vi) as mídias (suprimentos) serão adquiridas pela **Garín**, sempre que necessário.

13. Verificação e teste de restauração: sempre que possível o software de *backup* será configurado para verificar automaticamente o *backup*. A verificação será realizada por meio da comparação do conteúdo da cópia de segurança com os dados no disco.

14. Também deverão ser observados os processos e procedimentos estabelecidos no Código de Conduta, no capítulo de Política de Segurança Cibernética da Informação.

Efetiva Contingência

15. Na constatação de cenário classificado como "alto" será acionando o presente Plano de Contingência, sendo o Diretor de Compliance responsável por colocá-lo em prática e comunicar os clientes e o mercado acerca do eventos e das medidas adotadas para regularização das atividades da Sociedade.

16. Na impossibilidade de se utilizar o espaço físico do escritório, os Colaboradores da Sociedade poderão continuar trabalhando em suas próprias casas, através de Notebooks autorizados, internet banda larga e telefone,.

17. A **Garín** conta com acesso remoto aos seus bancos de dados virtuais disponível a todos os colaboradores autorizados pelo Diretor de Compliance.

18. A Sociedade possui smartphones próprios, devidamente autorizados, e com acesso à Internet móvel para qualquer eventualidade além de conexão com Internet de banda-larga diferente (NET Virtua, banda larga). A **Garín** possui também sistema de rede sem fio em todos os departamentos.

19. O serviço de e-mail da **Garín** é garantido por parceiro que provém suporte 24/7, serviço de AntiSpam, antivírus, recuperação de informação, site de recuperação de desastre e alertas relacionados ao vazamento de informações confidenciais e privilegiadas. A **Garín** utiliza ainda o Microsoft 365, que possibilita o acesso remoto de todas as mensagens pelos Colaboradores.

20. A **Garín** conta com 2 operadoras de telefone (MundVox e TransitTelecom). Em caso de falhas nas linhas telefônicas, os colaboradores da **Garín** ainda possuem celulares que podem substituir a telefonia fixa.

21. As informações do portfólio além de estarem nos sistemas internos da **Garín** são disponibilizadas diariamente pelo administrador, que também informará qualquer movimentação no passivo dos fundos para adequação do caixa dos fundos.

22. Em caso de falha de fornecimento de energia, a **Garín** possui nobreak (SMS) para suportar o funcionamento de seus servidores, rede corporativa, telefonia e de outros quatro estações de trabalho (desktops) para a efetiva continuidade dos negócios.

23. Em caso de efetiva necessidade de utilização da estrutura de contingência, deverão ser encaminhadas para o local de contingência as pessoas responsáveis pelas funções de: (i) boletagem das operações; (ii) gestão das carteiras; e (iii) comunicação com os administradores e Diretor de Compliance.

24. O serviço de e-mail da **Garín** é garantido por dispositivo de segurança SonicWALL que encontra-se instalado entre o roteador e a borda do link de internet, e oferece gerenciamento unificado de ameaças com função de firewall, proteção de conteúdo, antivírus, proteção contra invasões, inteligência de aplicativos, AntiSpam, filtragem de conteúdo e SSL VPN em uma única plataforma de hardware.

25. Com seus procedimentos de *backup* externo e acesso remoto a e-mails, a **Garín** pode continuar a funcionar mesmo que não possa ter acesso físico ao escritório.

26. Para a retomada célere e eficaz das operações após uma contingência, o Diretor de Compliance da Sociedade deve adotar as seguintes medidas, conforme o caso: (i) monitorar o escritório na reocupação; (ii) verificar a ausência de efeitos pós-desastre e de possíveis ameaças; (iii) garantir que todos os serviços de infraestrutura como, energia, água, telecomunicação, segurança, estão operacionais; (iv) instalar novos softwares e hardwares; (v) garantir bom funcionamento dos equipamentos de informática e comunicação, como também dos sistemas operacionais para assegurar completa funcionalidade; (vi) finalizar o Plano de Contingência em até 02 semanas; e (vii) coordenar o retorno dos integrantes da equipe para o escritório original.

Documentação

27. Deverá ser mantida no local de contingência uma lista com as informações de todos os integrantes da **Garín**, das corretoras com as quais se realizam negócios, os clientes e os prestadores de serviço contratados.

Atualização

28. As políticas e processos referentes no presente Plano de Contingência são revisados ao menos uma vez por ano e atualizados sempre que necessário. Também em uma base anual, os Colaboradores da Sociedade tem treinamento sobre o referido plano e suas eventuais atualizações.