PLANO DE CONTINUIDADE DE NEGÓCIOS

Siguler Guff Gestora de Investimentos (Asset Management) Brasil Ltda.

1.0

July / 2016

1. OBJETIVO

Este Plano de Continuidade de Negócios ("**PCN**") da Siguler Guff Gestora de Investimentos (Asset Management) Brasil Ltda. ("**SG Brasil**") tem por objetivo definir as estratégias de continuidade de negócios em caso de ocorrência de desastres ou incidentes de grandes proporções que provoquem a interrupção dos processos ou indisponibilidade física e lógica dos recursos e atividades da SG Brasil.

O uso pretendido do PCN é minimizar o impacto de um acontecimento inesperado que poderia apresentar inacessibilidade às instalações da SG Brasil.

Todas as menções ao Diretor de Compliance contempladas neste Manual se referem especificamente ao indivíduo presente em São Paulo. A SG Brasil recebe apoio das áreas e departamentos da Siguler Guff & Company ("**Siguler Guff**"), localizados em Nova York.

2. PREMISSAS

O PCN da SG Brasil tem como base as seguintes premissas:

(i) Notificação
(ii) Implementação
(iii) Preparação

I. NOTIFICAÇÃO

Na hipótese de o PCN precisar ser implementado, cada funcionário será notificado por telefone como parte do processo da árvore telefônica da Siguler Guff e da SG Brasil. Além disso, um email será enviado a todos os sócios, funcionários, estagiários e trainees ("**Colaboradores**") da SG Brasil, bem como contas pessoais (se possível). Considerando que o serviço de e-mail da SG Brasil pode ficar temporariamente comprometido, os Colaboradores devem verificar suas contas pessoais de e-mail, além de estarem disponíveis para receber uma ligação telefônia para receber instruções.

Determinados Colaboradores na árvore telefônica são designados "Autores de Chamadas". Os Autores de Chamadas serão responsáveis por telefonar para os demais funcionários na empresa e reportar à pessoa acima deles na árvore telefônica se o contato foi realizado. Os Autores de Chamadas nomeados devem certificar-se de ter os números de telefone residencional e celular dos funcionários em listas prontamente disponíveis.

II. IMPLEMENTAÇÃO

Caso os Colaboradores não possam acessar fisicamente o escritório, ou caso a estrutura do escritório esteja severamente comprometida, o PCN será ativado. Este plano envolve 3 (três) componentes tecnológicos fundamentais:

- **Citrix**
  O Citrix permitirá que os Colaboradores acessem com segurança aplicações como se eles estivessem em suas áreas de trabalho. Os Colaboradores com computadores *desktop* podem usar o *Remote Desktop Client* da Microsoft para controlar remotamente o seu PC do escritório.

- **VPN**
  Os Colaboradores com laptops providenciados pela empresa terão o cliente VPN ("**Virtual Private Network**") instalado, permitindo o acesso remoto ao e-mail e ao servidor de arquivos. Embora outras aplicações de laptops instaladas poderão ser executadas, é recomendável aos Colaboradores que usem o Citrix para acesso mais rápido.

- **Webmail (OWA)**
  Para os Colaboradores que precisam apenas de acesso ao e-mail, o cliente OWA é o ideal e funciona em qualquer navegador da web.

Todos os Colaboradores devem garantir que seus computadores domésticos possam executar o Citrix (ou o VPN, se tiverem acesso), acessando o sistema periodicamente de suas residências.

Alguns Colaboradores podem ser solicitados a reportar-se a outros escritórios da Siguler Guff. Esta decisão será tomada caso-a-caso e a notificação e os detalhes serão fornecidos por um gerente ou supervisor, se necessário.

Caso o escritório da Siguler Guff em Nova York esteja comprometido (por exemplo, por queda de energia), a administração deverá decidir sobre a necessidade ou não de uma transferência (*failover*) para o escritório da Siguler Guff em Boston.

III. PREPARAÇÃO

A preparação dos seguintes itens deve ser feita com antecedência:

- Manter uma cópia deste PCN na residência do Colaborador e em sua mesa no escritório.
- Se um Colaborador for designado "Autor de Chamadas", tal Colaborador deverá armazenar os números de telefone dos funcionários nomeados para facilitar a referência.
- Testar periodicamente a capacidade de acessar a rede da SG Brasil via Citrix ou VPN.

3. CENÁRIO DE CONTINGÊNCIA

Adotamos como cenário de contingência a indisponibilidade total do uso das instalações tecnológicas ou dos escritórios em caso de desastre de grandes proporções, tais como, mas não limitados a, incêndios não controlados, bombas de alto poder de destruição, entre outros, ou indisponibilidade de alguma das aplicações críticas de negócio.

4. ACIONAMENTO DO PCN

Deliberado pelo acionamento do PCN, as equipes da SG Brasil irão realizar (i) comunicação verbal, em caso de ocorrência de desastre durante o expediente regular; e (ii) contato telefônico, em caso de ocorrência de desastre em horários em que as equipes não estiverem nas dependências da SG Brasil.

Em ambos os casos, será responsabilidade do presidente do escritório de São Paulo acionar sua equipe. Em caso de indisponibilidade do presidente, a comunicação será feita pelo Diretor de Compliance.

Além disso, o Diretor de Compliance deverá avaliar a necessidade de comunicar parceiros e órgãos reguladores sobre o estado de contingência e as formas de contato com a SG Brasil. Caso necessário, essas informações serão disponibilizadas em nosso site e encaminhadas via e-mail aos sócios e órgãos reguladores.

5. RECUPERAÇÃO EMERGENCIAL

5.1 CENARIO DE INDISPONIBILIDADE DOS SITES

As atividades críticas da SG Brasil se encontram localizadas nos datacenters da Siguler Guff em Nova York (principal) e da Siguler Guff em Boston (backup). Os sistemas críticos e links de comunicação estão duplicados e sincronizados nos datacenters.

A SG Brasil utiliza o datacenter principal nos escritórios da Siguler Guff em Nova York e em casos de contingência e indisponibilidade do datacenter de Nova York, todas as atividades realizadas serão redirecionadas para o escritório da Siguler Guff em Boston.

No caso de indisponibilidade de um datacenter, as equipes-chave de suporte e de infraestrutura serão acionadas de modo a preparar os sistemas de dados de contingência, bem como a

estrutura tecnológica, permitindo que as demais equipes-chave retomem a continuidade de seus processos no menor tempo possível.

5.1.1 RECUPERAÇÃO DAS ATIVIDADES DOS DATACENTERS

A recuperação será deliberada pela equipe de administração da Siguler Guff após a análise da extensão do desastre e do tempo necessário para o restabelecimento das condições normais de trabalho.

Nesse cenário o tempo de inatividade será mínimo, graças aos sistemas críticos e links de comunicação ativos entre os escritórios da Siguler Guff em Nova York e Boston.

5.2 CENÁRIO DE INDISPONIBILIDADE DE ESCRITÓRIOS

No caso de indisponibilidade dos escritórios da SG Brasil, onde são realizadas as atividades críticas e imprescindíveis para a continuidade dos negócios, as equipes-chave poderão acessar remotamente estações de trabalho virtuais através da conexão VPN.

5.2.1 RECUPERAÇÃO DAS ATIVIDADES DOS ESCRITÓRIOS

A recuperação será deliberada pela equipe de administração da Siguler Guff após a análise da extensão do desastre e do tempo necessário para o restabelecimento das condições normais de trabalho.

5.3 CENÁRIO DE INDISPONIBILIDADE DAS APLICAÇÕES CRÍTICAS

No caso de indisponibilidade de alguma das aplicações críticas do negócio devido à falta prolongada de energia elétrica durante horários críticos ou danos (intencionais ou não) em algum equipamento dentro dos sites, a SG Brasil dispõe de métodos alternativos para a execução dos negócios até conseguir restabelecer suas atividades com normalidade.

5.3.1 RECUPERAÇÃO DAS APLICAÇÕES CRÍTICAS

A recuperação será deliberada pela equipe de administração da Siguler Guff após análise da extensão do desastre e do tempo necessário para o reestabelecimento das condições normais de trabalho.

A recuperação contemplará as ações para retomada das atividades das áreas críticas e das áreas de recuperação estratégica, dependendo da aplicação indisponível.

6. RETORNO À NORMALIDADE

O retorno à normalidade nos cenários de indisponibilidade são os processos de (i) planejamento e implementação de procedimentos para o reparo, realocação ou compra/aluguel de ativos da instituição; (ii) recuperação do datacenter indisponível ou migração para um novo datacenter que esteja disponível; e (iii) busca por um novo local para as atividades da instituição, caso o escritório principal não possa ser recuperado.

A administração sênior decidirá se será iniciada a busca por um novo local para as atividades da SG Brasil ou se deverá esperar pela recuperação do local atingido pelo desastre.

7. TESTES E PRAZO DE ATUALIZAÇÃO DO PCN

Anualmente, o Diretor de Compliance da SG Brasil, em conjunto com as áreas de Compliance e Jurídico, Operações e Tecnologia, realizará testes para avaliar a adesão aos procedimentos do PCN para garantir a prontidão dos funcionários na eventualidade de um desastre, além de assegurar que os procedimentos do PCN estão atualizados. Estes testes poderão incluir: (i) testes de árvore telefônica para confirmar que as informações de contato de emergência para os escritórios da SG Brasil e da Siguler Guff estão precisos e atualizados em WebCRD; (ii) realizar treinamento para os funcionários sobre alterações e/ou atualizações relacionadas ao PCN; (iii) testes de backup de servidor de e-mail em caso de falha; e (iv) testes de “condições ruins de clima”, para que vários funcionários acessem o sistema e trabalhem de suas residências para confirmar a inexistência de problemas com acessos remotos.

São de responsabilidade da equipe de Operações da SG Brasil o cumprimento do teste anual, o acompanhamento e validade do teste realizado, bem como a atualização do PCN.

O PCN será revisto, no mínimo, anualmente para garantir a eficiência das estratégias dos processos de recuperação.

8. FORMALIZAÇÃO DOS TESTES

Para a realização dos testes, o Diretor de Compliance e a área de Compliance da Siguler Guff irão monitorar os resultados dos testes, no mínimo, anualmente, incluindo a documentação das datas dos testes, de um breve resumo e dos resultados dos testes.