PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Este Plano de Contingência e de Continuidade de Negócios da PDG Companhia Securitizadora ("Plano" e "SEC", respectivamente) integra o Manual de Regras, Procedimentos e Controles Internos da SEC ("Manual de Compliance") e foi elaborado em cumprimento à Resolução CVM 60, de 23 de dezembro de 2021 ("Resolução 60").

O Plano tem por objetivo estabelecer as medidas de contingência, continuidade de negócios e recuperação de desastres que assegurem a continuidade das atividades da SEC e a integridade das informações sob sua responsabilidade, bem como de interfaces com sistemas de terceiros, que permitam à SEC reassumir o processamento das operações em um intervalo de tempo adequado às necessidades e dinâmica do negócio. As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores da SEC.

1. Riscos em Potencial

Os principais riscos aos quais a SEC está sujeita são aqueles relacionados ao uso adequado de suas instalações e ferramentas, incluindo: (i) falhas de energia; (ii) falhas de acesso à internet; (iii) ataques cibernéticos; e (iv) eventos que impeçam o acesso físico à SEC, incluindo eventos da natureza.

2. Principais Situações Contingenciais Identificadas e Medidas Preventivas

A SEC atua por meio de rotinas preventivas e corretivas elaboradas e/ou implementadas para assegurar a continuidade das suas atividades e a minimização de prejuízos próprios e/ou dos patrimônios separados por contingências.

Sem prejuízo, fazemos referência aos demais capítulos do Manual de Compliance para mais informações sobre confidencialidade, sigilo e segurança da informação, treinamentos e outros.

2.1. Segurança da Informação e Vazamento:

As medidas de segurança da informação e treinamentos, realizados em paralelo a testes de intrusão, testes de *phishing* periódicos e varreduras de vulnerabilidades realizados pelo departamento de tecnologia e segurança da informação do Grupo PDG, devem ser observadas por todos os colaboradores.

Todo acesso a diretórios e sistemas de informações da SEC será objeto de controles de acesso. Somente poderão acessar os referidos diretórios e sistemas de informação aqueles colaboradores previamente autorizados pelo Diretor responsável pelo cumprimento das regras, políticas, procedimentos e controles internos ("*Compliance*").

O controle do acesso a sistemas de informações da SEC levará em conta as seguintes premissas:

(i) Garantia de que o nível de acesso concedido ao colaborador é adequado ao seu perfil; e

(ii) Cancelamento imediato do acesso concedido a colaboradores desligados, afastados ou que tenham sua função alterada na SEC. Nesse último caso, o Diretor responsável por *Compliance* da SEC deverá conceder uma nova autorização ao colaborador que teve sua função alterada para o devido acesso ao sistema de informações.

Os Colaboradores deverão comunicar ao Diretor responsável por *Compliance* da SEC quaisquer casos de violações às normas de segurança da informação que tenham conhecimento. Toda violação ou desvio será investigado para a determinação das medidas necessárias, visando à correção da falha, ou reestruturação de processo.

Em caso de vazamento de informação confidencial, o Diretor responsável por *Compliance* da SEC discutirá com a equipe interna de tecnologia da informação, ou com funcionários terceirizados e contratados para essas funções, qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos, levando o assunto aos demais membros da Administração da SEC, conforme o caso.

2.2. Infraestrutura e E-mails:

A SEC tem uma rede integrada de computadores, revisados quanto à capacidade, segurança e nível de atualização de seus componentes, com o suporte técnico de empresa terceirizada contratada. Ainda, serão realizados *backups* em servidores, e são adotados procedimentos contínuos relacionados aos antivírus, responsáveis por proteger, sem interrupção, a rede interna de computadores, seus dados e os dos patrimônios separados.

Em complemento, a SEC tem seu servidor de e-mails é hospedado junto a Microsoft, o que garante alta disponibilidade e segurança, viabilizando o trabalho remoto e via computadores reserva, se e quando necessário, bem como a manutenção de registros para auditorias e inspeções.

2.3. Sistemas Críticos:

Os sistemas Aztronic e SAP são considerados críticos para as atividades da SEC, de modo que, visando garantir a continuidade das atividades quando da materialização de eventos de riscos, alguns colaboradores, mediante autorização, poderão ter acesso aos referidos sistemas críticos de forma remota (acesso em casa), mediante prévia e expressa autorização do Diretor responsável por *Compliance* da SEC.

2.4. Testes de Capacidade Operacional:

Anualmente, a SEC realizará testes de eficiência e rapidez de acesso para garantir que os sistemas estão aptos a operar de forma remota. A atualização e bom estado das cópias mantidas na sede da SEC e em meio digital também serão verificados.

2.5. Recuperação de Atividades:

O Diretor responsável por Compliance será responsável por verificar a volta à normalidade das instalações físicas da securitizadora, observando-se quando: (i) as instalações estiverem em condições de serem utilizadas; (ii) não há risco para os colaboradores para regresso às instalações; (iii) há condições de serem desenvolvidos os procedimentos habituais de

trabalhos; e (iv) o departamento de tecnologia e segurança da informação do Grupo PDG, estiver pronto para iniciar o processo de retorno, verificando equipamentos, restaurando os acessos na rede, restabelecendo os acessos de código de segurançaAinda, todos os colaboradores que permaneceram em suas residências ou em local designado pelo Diretor responsável por *Compliance* da SEC serão por ele avisados para o retorno às instalações da SEC.

3. Responsabilidade

Abaixo apresentamos informações cadastrais do Diretor responsável por *Compliance* e pelo cumprimento do Plano:

Nome	**Roberto Giarelli**
E-mail	roberto.giarelli@ixincorporadora.com.br>
Telefone	(11) 2110-4800

4. Atualização

Este Plano será submetido à revisão anual ou em períodos inferiores a este, sempre que o Diretor responsável por *Compliance* considerar necessário, com o intuito de preservar as condições de segurança para a SEC e para os patrimônios separados.

Versão	Data	Responsabilidade
1	28/10/2022	Roberto Giarelli