contato@austrocapital.com.br
www.austrocapital.com.br

PLANO DE GESTÃO E CONTINUIDADE DE NEGÓCIOS

Versão 4.0
Revisado em: 08/02/2021

Atividade	Área
Elaboração	Área de *Compliance*
Revisão	Diretor de *Compliance* e Riscos
Aprovação	Diretor de *Compliance* e Riscos

Classificação das Informações
[ ] Uso Interno [X] Uso Público

1. Introdução, Objetivo e Abrangência

Este Plano de Gestão e Continuidade de Negócios ("PCN") se aplica às administradoras de carteiras de títulos e valores mobiliários, na modalidade gestora de recursos, nos termos da Instrução editada pela Comissão de Valores Mobiliários ("CVM") nº 558, de 26 de março de 2015 ("ICVM 558"), conforme alterada, do Grupo Austro, quais sejam, Austro Gestão de Recursos Ltda ("Austro Gestão"), Axis Capital Gestão de Recursos Ltda. ("Axis Capital") e a Alummini Gestão de Recursos Ltda. ("Alummini Gestão"). Quando referidas em conjunto no presente documento, Austro Gestão, Axis Capital e Alummini Gestão são designadas "Gestoras".

Pelo presente documento, o Grupo Austro, vem, nos termos da ICVM 558, e do Código da Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais ("ANBIMA"), definir seu PCN que estabelece estratégias e procedimentos a serem observados na eventualidade de incidentes ou situações de emergência que envolvam o Grupo Austro e/ou seus sócios, diretores, empregados, funcionários, *trainees*, estagiários, prestadores de serviços que venham, de maneira direta ou indireta, trabalhar para o Grupo Austro e todos que, de alguma forma, auxiliam o desenvolvimento das atividades do Grupo Austro ("Membros").

Em decorrência disto, é entendimento corrente que o bem mais precioso do Grupo Austro é o patrimônio dos clientes sob gestão e as informações estratégicas decorrentes, com inequívoca prioridade sobre os ativos organizacionais. Portanto, assegurar aos clientes que os seus patrimônios não serão afetados por eventos cujo grau de previsibilidade seja nulo, mas de altíssimo impacto nas operações organizacionais mais críticas, é a essência e objetivo principal do trabalho em curso.

O uso pretendido do PCN é minimizar o impacto de um acontecimento inesperado que poderia apresentar inacessibilidade às instalações da Grupo Austro. Todas as menções ao Diretor de *Compliance* e Riscos, conforme definido no contrato social vigente de cada uma das Gestoras, contempladas neste PCN, se referem especificamente ao indivíduo presente em Porto Alegre.

Por fim, recomenda-se a leitura deste PCN em conjunto com a Política de Segurança da Informação, Confidencialidade, Segregação e Segurança Cibernética, sobretudo em decorrência das regras estabelecidas pelo Grupo Austro para garantir a devida segregação entre as Gestoras.

2. Objetivos Gerais e Específicos

Como estratégia para atingir nosso objetivo principal, definimos como objetivos específicos:

a) Realizar *backup* externo e diário de todo o banco de dados, envolvendo todas as operações diárias, incluindo os arquivos de programas;

b) Assegurar a integridade, segurança, qualidade, confidencialidade e acessibilidade dos dados e informações;

c) Manter os sistemas operacionais disponíveis;

d) Manter rede eletrônica em funcionamento e em boas condições operacionais.

Para redução e controle de eventuais perdas com contingências, todos os Membros do Grupo Austro deverão conhecer os procedimentos de *backup* e salvaguarda de informações (confidenciais ou não), planos de evacuação das instalações físicas e melhores práticas de saúde e segurança no ambiente de trabalho.

3. Análise de Risco

Definimos como foco o desenvolvimento de um plano de ação que assegure a continuidade das atividades operacionais no Grupo Austro mesmo nos eventos de maior ruptura operacional, independentemente do se seu nível de risco de ocorrência. Outra consideração que fundamenta a opção do Grupo Austro por analisar risco sobre os recursos abaixo, prende-se ao objetivo exclusivo de manter ou restabelecer rapidamente a gestão e controle do patrimônio dos clientes.

Utilizamos como conceito de risco: “sendo a probabilidade de ocorrência de um evento indesejado e ou imprevisível causando graves rupturas operacionais e consequente prejuízo patrimonial”.

RISCO = Probabilidade do Evento x Consequência

Assim nossa análise de risco concentra-se em avaliar eventos que provoquem danos aos recursos abaixo:

a) Segurança, integridade, qualidade e acessibilidade aos dados e informações;
b) Corpo técnico;
c) Tecnologia das informações;
d) Instalações.

A avaliação dos riscos aos quais o Grupo Austro, na execução das suas atividades cotidianas, se expõe, podem analisada sob três aspectos:

I) A **PROBABILIDADE** de que o evento produza rupturas graves;
II) A GRAVIDADE das possíveis consequências prejudiciais;
III) O ÍNDICE de exposição aos riscos.

A probabilidade de consequências prejudiciais aumenta com a maior exposição. Por isso, a exposição deve ser considerada como outra dimensão de probabilidade. A avaliação de riscos considera a probabilidade e a gravidade da consequência prejudicial, determinando o potencial de perdas.

PROBABILIDADE DO EVENTO		
Definição Qualitativa	**Significado**	**Pontuação**
Frequente	Ocorrência provável (evento frequente)	5
Ocasional	Provável que ocorra (eventos ocasionais)	4
Remoto	Improvável, porém possível de ocorrer (ocorre raramente)	3
Improvável	Muito improvável que ocorra (sem registros de eventos anteriores)	2
Extremamente Improvável	Quase inconcebível que o evento ocorra	1

Avaliada a probabilidade de ocorrência do evento, passamos a avaliar a severidade das consequências do evento que regem o grau de urgência da medida de segurança operacional requerida.

SEVERIDADE DOS EVENTOS		
Definições	**Significado**	**Classificação**
Gravíssimo	Destruição de Equipamentos e Instalações. Mortes múltiplas.	A
Grave	Destruição de Equipamentos. Instalações inacessíveis.	B
Médio	Equipamentos parcialmente comprometidos. Acessos limitados.	C
Baixo	Instalações e Equipamentos operacionais. Uso alternativo de redes.	D
Insignificante	Consequências leves.	E

partir da análise de probabilidade e severidade dos eventos podemos construir uma matriz de avaliação de riscos, como a que se apresenta abaixo, que é a ferramenta utilizada para ordenar em grau de prioridade os riscos que requerem mais atenção.

SEVERIDADE DO RISCO					
PROBABILIDADE DO RISCO	Gravíssimo A	Grave B	Médio C	Baixo D	Insignificante E
Frequente - 5	5A	5B	5C	5D	5E
Ocasional - 4	4A	4B	4C	4D	4E
Remoto - 3	3A	3B	3C	3D	3E
Improvável - 2	2A	2B	2C	2D	2E
Extremamente improvável - 1	1A	1B	1C	1D	1E

Com base nas avaliações de riscos podemos ordená-los por prioridade orientada pelos critérios de aceitabilidade dos riscos.

Aceitável – quando não é necessário adotar medidas mitigatórias, a menos que se possa reduzir mais o risco com pouco custo ou esforço;

Tolerável – a organização está preparada para suportar o risco. Medidas mitigatórias são recomendadas;

Intolerável – condições que impliquem em cessar as operações até que o risco se reduza ao nível tolerável.

GESTÃO DE RISCO	ÍNDICE DE AVALIAÇÃO DE RISCO	CRITÉRIO DE ACEITABILIDADE
Intolerável	5A; 5B; 5C 4A; 4B; 3A	Inaceitável sob as circunstâncias existentes
Tolerável	5D; 5E; 4C; 4D 4E; 3B; 3C; 3D 2A; 2B; 2C	Aceitável com mitigação de risco. Pode requerer uma decisão direta
Aceitável	3E; 2D; 2E; 1A 1B; 1C; 1D; 1E	Aceitável

Não existe 100% (cem por cento) de segurança operacional absoluta. São necessárias ações continuadas com objetivo de manutenção dos riscos nos seus mais baixos níveis. Em considerando um determinado risco intolerável ou tolerável, faz-se necessário a adoção de

medidas mitigadoras. Quanto mais elevado o risco, maior a urgência. A redução de risco se dá pela redução da gravidade das consequências, da probabilidade ou da exposição.

O Grupo Austro tem de forma consolidada algumas ações mitigatórias de risco, que buscam assegurar sua operacionalidade, permitindo que os riscos a que se expõe – cenários abaixo – sejam classificados como "toleráveis":

a) "*Backup*" externo, diário e automático, com redundância em equipamentos localizados fora do continente onde o Grupo Austro opera;

b) "*Backup*" extensivo a todos os aplicativos e arquivos de programas em uso na organização (incluindo registro dos e-mails);

c) "Data Center" contratado, permitindo comunicação e acesso remoto para dados, aplicativos e arquivos de programa;

d) Toda a documentação que represente obrigações e haveres do Grupo Austro é digitalizada, respeitadas as regras de segregação lógica entre as Gestoras, detalhadas na Política de Segurança da Informação, Confidencialidade, Segregação e Segurança Cibernética;

e) Todos os documentos, arquivos e pastas criadas, usadas e/ou atualizadas no dia a dia são automaticamente salvas no servidor para posterior "*backup*";

f) A área de *compliance* mantém registro atualizado de todas as senhas de acesso aos *softwares* de gestão usados no Grupo Austro;

g) Contrato terceirizado de manutenção de TI com presença rotineira no Grupo Austro e atendimento especial em casos de necessidade;

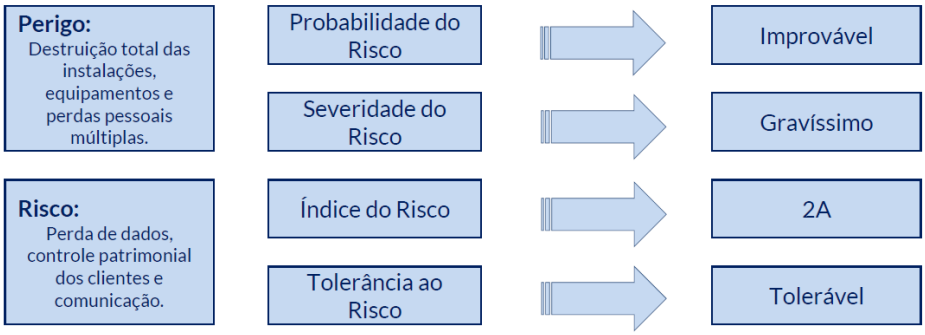
h) Redundância no serviço de internet (duas operadoras contratadas simultaneamente), evitando o risco de o sistema ficar fora do ar.

4. Identificação de Eventos X Riscos

Ao avaliarmos os eventos possíveis, sempre focamos em efeitos que possam comprometer dados e informações sobre o patrimônio dos clientes, pessoas, informática e comunicação e instalações físicas. Estes são os mais importantes – imprescindíveis – fatores de continuidade dos negócios no Grupo Austro.

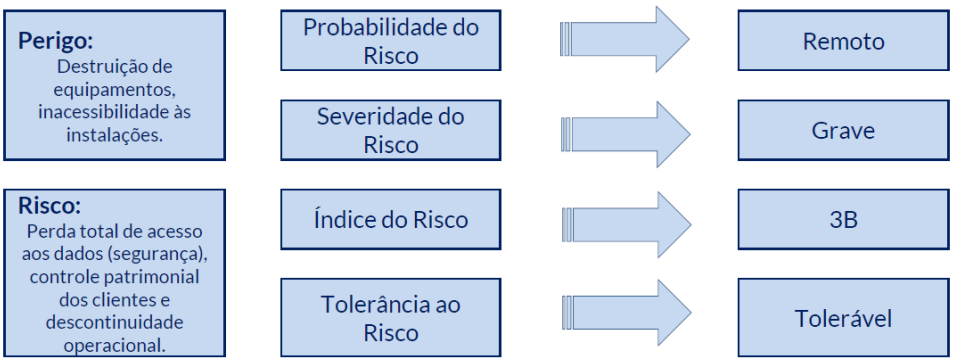
4.1. Cenário 1

Ocorrência de eventos naturais e ou acidente de grandes proporções com sérios danos nas instalações físicas, equipamentos de informática, sistema de comunicação e perdas pessoais múltiplas.



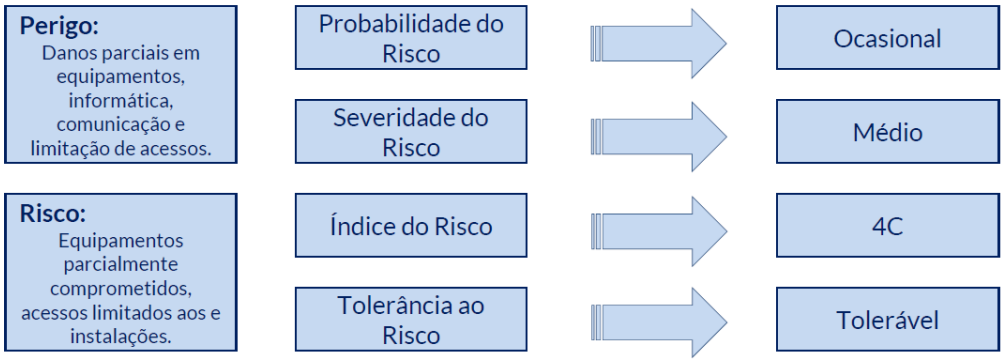
4.2. Cenário 2

Acidente no entorno das instalações e ou distúrbios sociais de grandes proporções ocasionando destruição de equipamentos e ou tornando as instalações inacessíveis.

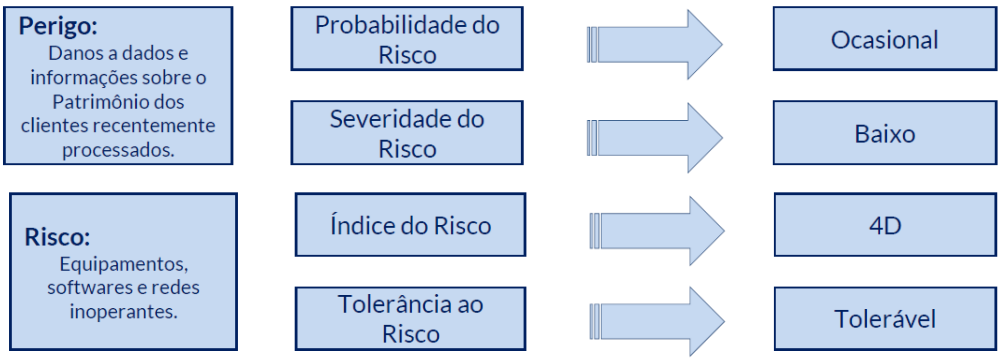


4.3. Cenário 3

Evento acidental provocando danos parciais nos equipamentos, com comprometimento parcial dos sistemas de informática e de comunicação, provocando limitações e restrições de acesso às instalações físicas.



Em caso de acidente originado por causas naturais ou humanas em que haja interrupção no fornecimento de energia por tempo muito superior ao de suporte dos “no breaks”, causando ruptura no funcionamento dos equipamentos e redes de comunicação.



5. Plano de Administração de Crise (PAC)

Neste tópico mapeamos os procedimentos planejados e que serão adotados enquanto perdurar a situação de crise, até a total normalidade operacional da organização. Definimos também um passo a passo de todas as ações desde a “declaração de situação de emergência” à execução das ações que vise retomada imediata das operações em todas as áreas do Grupo Austro.

O Grupo Austro, conforme exposto anteriormente, é formado pelas Gestoras e mantem suas operações num espaço total de 106,77 m² (sento e seis metros quadrados e setenta e sete centímetros, observadas as regras de segregação consolidadas na Política de Segurança da Informação, Confidencialidade, Segregação e Segurança Cibernética. Após analisados os riscos a que se expõe são toleráveis com mitigação, o PAC terá a simplicidade e funcionalidade adequada.

5.1. O que é Essencial para a Manutenção das Operações do Grupo Austro?

Pela peculiaridade operacional do Grupo Austro prestar serviço de administração de carteiras de valores mobiliários, exclusivamente na categoria "gestor de recursos", nos termos da ICVM 558, onde a guarda de valores, títulos, registros e precificação de ativos são operações externas, realizadas por Bancos Custodiantes, define-se como essencial às operações do Grupo Austro o que segue:

a) Pessoas em geral, com atenção especial aos gestores, *back office* e *risk control*;
b) Segurança, integridade e acessibilidade dos dados e informações referentes ao patrimônio dos clientes;
c) Redes de comunicação de dados e voz;
d) *Softwares* de gestão e controles;
e) *Hardwares* compatíveis com as exigências operacionais dos *softwares* e redes;
f) Recuperação dos dados e informações geradas nas últimas 24 horas anteriores ao evento de ruptura operacional.

5.2. Central de Crise

Em caso de evento com rupturas operacionais será instalada uma central de crise em local determinado pelo Conselho de Administração, de fácil acesso a todos os Membros da organização.

5.3. Pessoas e Ações

A implementação dos planos de contingência deverá ser realizada em até quatro horas e será de responsabilidade do Diretor de *Compliance* e Riscos, observadas as atribuições adiante:

Diretor de *Compliance* e Riscos

- Declaração de crise operacional e coordenação do PAC;
- Verificar e validar a segurança, integridade e acessibilidade dos dados capturados e arquivados pelo sistema de "*backup*" diário;
- Ativar serviços de TI contratados previamente;
- Ativar técnicos responsáveis por manutenção e funcionalidade dos *hardwares* e *softwares*.

Compliance Officer

- Garantir pleno funcionamento da Política de Segurança de TI, inclusive com fornecimento emergencial de equipamentos completos: desktops e notebooks com as especificações abaixo:

- Adquirir em regime de urgência, no mínimo 04 (quatro) modens banda larga que restabeleça, mesmo que precariamente, as comunicações via rede.

Gestores, Back Office e Risk Control

- Atualizar e ou recuperar dados e informações não capturados no último "*backup*" disponível no "Data Center";
- Dar continuidade as operações.

5.4. Testes de Contingências

Os testes de contingências possibilitam que o Grupo Austro esteja preparado proporcionando condições adequadas para continuar suas operações. Sendo assim, anualmente, no mês de abril, é realizado pela equipe de Suporte de TI um teste de contingência para verificar:

- Acesso aos sistemas;
- Acesso ao e-mail corporativo;
- Acesso aos dados armazenados; e
- Qualquer outra atividade necessária para continuidade do negócio.

O resultado do teste é registrado em relatório baseado no modelo disponibilizado pela ANBIMA, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento do plano de continuidade de negócios.

6. Disposições Finais

Este PCN será revisado, no mínimo, anualmente. Não obstante as revisões estipuladas, poderá ser alterado sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

Este PCN se aplica ao Grupo Austro.

A área de *compliance* informará oportunamente aos Membros sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página das Gestoras na rede mundial de computadores.

Este PCN revoga todas as versões anteriores e passa a vigorar na data de sua aprovação.