AUSTRIA | CAPITAL

GESTÃO DE RECURSOS

Manual de Governança, Controles Internos e Compliance

SUMÁRIO

1. OBJETIVO

O presente Manual de Governança, Controles Internos e Compliance ("Manual") tem por objetivo estabelecer as diretrizes e procedimentos que orientam a atuação da Austria Capital Gestão de Recursos, assegurando a eficácia de seu sistema de controles internos e a conformidade de suas atividades com a legislação e regulamentação aplicáveis.

As regras e práticas aqui previstas visam garantir padrões de ética, integridade e profissionalismo, promovendo a cultura de controles internos e de conformidade, em linha com o disposto na Resolução CVM nº 21, bem como nas demais normas que regem a atividade de administração de carteiras de valores mobiliários.

Além disso, visa garantir a aderência contínua às normas internas e externas relacionadas à atividade de administração de carteiras de valores mobiliários, assegurando padrões elevados de governança, transparência, conduta profissional e gestão de riscos operacionais, legais e reputacionais.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os indivíduos que mantenham vínculo com a Austria Capital Gestão de Recursos, independentemente da natureza jurídica ou formal de sua relação. Estão abrangidos, para fins desta Política, os sócios, administradores, colaboradores, empregados, prestadores de serviço, consultores, representantes, estagiários e quaisquer terceiros que atuem em nome ou no interesse da sociedade.

A observância das diretrizes aqui estabelecidas é obrigatória no exercício de qualquer atividade relacionada à administração de carteiras de valores mobiliários, bem como em todas as interações internas e externas que envolvam a atuação da Austria Capital Gestão de Recursos no mercado financeiro, assegurando a conformidade com os padrões regulatórios, éticos e profissionais exigidos pelo setor.

3. DIRETRIZES

Este Manual tem como diretrizes:

a) Disseminar a cultura da importância dos controles internos entre todos os colaboradores da Austria Capital Gestão de Recursos;
b) Garantir o cumprimento das normas regulatórias e das políticas e procedimentos internos;
c) Estruturar os controles internos em linha com os objetivos do negócio e com os riscos inerentes à atividade;
d) Definir de forma clara as responsabilidades e níveis de autoridade, respeitada a estrutura organizacional da gestora;
e) Possibilitar a elaboração de relatórios sobre a situação dos controles internos, quando aplicável;
f) Estabelecer fluxos de aprovação de acordo com as alçadas definidas; e
g) Promover a revisão periódica dos processos de controles internos, assegurando seu constante aprimoramento.

4. ÁREA DE RISCO E COMPLIANCE

O Diretor de Risco e Compliance é responsável pela concepção, implementação e atualização contínua das políticas e controles internos da gestora. Suas atribuições abrangem a revisão periódica dos códigos, manuais e políticas internas; a implementação de controles internos; a realização de testes de aderência; e a promoção de treinamentos institucionais para todos os colaboradores.

Além disso, compete à Área de Risco e Compliance a supervisão da correta aplicação das normas e procedimentos internos, com o objetivo de mitigar riscos operacionais, legais, reputacionais e regulatórios. A área atua com total independência funcional, sem subordinação hierárquica a outras áreas da estrutura, inclusive à área de gestão.

Dentre as principais responsabilidades da Área de Risco e Compliance, destacam-se:

a) Assessorar tecnicamente as demais áreas sobre normas e regulamentações emitidos por órgãos reguladores e autorreguladores;
b) Identificar, avaliar e documentar os riscos de conformidade relacionados às atividades desenvolvidas pela gestora;
c) Zelar pela veracidade, integridade e tempestividade das informações disponibilizadas ao público, nos canais oficiais da gestora e nos sistemas dos órgãos reguladores e autorreguladores;
d) Realizar testes periódicos de efetividade dos controles internos, sugerindo e acompanhando planos de ação para eventual remediação;
e) Supervisionar os controles de acesso a sistemas, redes e o correto armazenamento de backups e registros eletrônicos;
f) Elaborar o Relatório Anual de Compliance, nos termos da regulamentação aplicável;
g) Supervisionar e atender às solicitações de órgãos reguladores, autorreguladores, auditorias externas e processos de *due diligence*;
h) Implementar e monitorar a Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo;
i) Acompanhar a evolução regulatória e autorregulatória, interpretando e implementando novas diretrizes quando necessário;
j) Promover treinamentos e ações de disseminação da cultura de compliance e ética.
k) Avaliar tecnicamente situações em que conflitos de interesse forem inevitáveis, propondo medidas mitigadoras.

5. POLÍTICA DE CONFIDENCIALIDADE

Informações confidenciais

A Austria Capital Gestão de Recursos estabelece regras para assegurar a confidencialidade, integridade e disponibilidade das informações próprias, de clientes, investidores, contrapartes e carteiras sob gestão.

Esta Política aplica-se a sócios, administradores, colaboradores, funcionários e terceiros com acesso autorizado e tem como objetivo proteger a Austria Capital Gestão de Recursos contra a divulgação indevida de informações confidenciais obtidas no exercício das atividades de administração de carteiras de valores mobiliários, bem como bem como contra o uso, cessão ou

divulgação não autorizada de informações, documentos, modelos, metodologias, estratégias, produtos ou serviços que representem propriedade intelectual da gestora.

Consideram-se Informações Confidenciais todas as informações não públicas, disponíveis em meio físico ou eletrônico, de natureza técnica, financeira, comercial, operacional ou estratégica, relacionadas à Austria Capital Gestão de Recursos, suas atividades, clientes ou carteiras geridas. Não se incluem informações que (i) já sejam de domínio público, desde que não em razão de violação desta Política; ou (ii) tenham sido legitimamente recebidas de terceiros autorizados à sua divulgação.

Consideram-se Informações Privilegiadas toda a informação relevante, não pública, cuja divulgação possa influenciar preços de valores mobiliários ou decisões de investimento.

Diretrizes

Todos os sócios, administradores, colaboradores, funcionários e terceiros com acesso autorizado devem:

a) Manter sigilo absoluto sobre quaisquer Informações Confidenciais, abstendo-se de utilizá-las ou divulgá-las sem autorização formal e restrita à finalidade profissional;
b) Reconhecer que materiais, documentos, modelos, estratégias ou ferramentas desenvolvidas no âmbito da Gestora constituem propriedade exclusiva da Austria Capital Gestão de Recursos, vedado o uso ou compartilhamento não autorizado;
c) Observar que o acesso a informações será concedido conforme a função desempenhada, mediante controles estabelecidos pela área de Risco e Compliance;
d) Limitar eventual divulgação de informações em cumprimento de obrigação legal ou determinação de autoridade competente ao estritamente necessário.

Procedimentos

O acesso a informações é concedido pelo princípio do menor privilégio, com credenciais individuais e registro de logs que possibilitem identificar usuários, ações e períodos. Em casos de alteração de função ou desligamento, os acessos são revisados e revogados de forma imediata. O detalhamento técnico desses procedimentos encontra-se no Manual de Segregação de Atividades e Confidencialidade.

São mantidas barreiras informacionais entre funções e atividades que possam gerar conflitos de interesse. O compartilhamento entre áreas depende de necessidade funcional e, quando aplicável, aprovação prévia do Diretor de Risco e Compliance.

Constituem condutas expressamente proibidas, sujeitas a medidas disciplinares e sanções legais, conforme previsto no Código de Ética:

a) uso indevido de informação confidencial e/ou privilegiada;
b) recomendações ou “dicas” que permitam a terceiros negociar com base em informação não pública;
c) front-running.

O compartilhamento de informações com terceiros somente ocorre mediante necessidade justificada, aprovação formal do Diretor de Risco e Compliance e assinatura de Acordo de Confidencialidade (NDA) com cláusulas de segurança equivalentes às internas. O registro das aprovações e dos Acordos de Confidencialidade é de responsabilidade da Área de Risco e Compliance.

Em caso de suspeita de violação ou vazamento de informações confidenciais, devem ser observados os procedimentos previstos na Política de Segurança da Informação da Austria Capital Gestão de Recursos.

O descumprimento desta Política poderá ensejar medidas internas corretivas, sem prejuízo de eventuais responsabilidades legais aplicáveis.

Caso qualquer colaborador tome conhecimento de violação desta Política por parte de terceiros ou colegas, deverá reportar imediatamente o fato à área de Risco e Compliance.

A área de Risco e Compliance é responsável por supervisionar o cumprimento desta Política, manter controles adequados de acesso, analisar eventuais exceções, adotar mecanismos eficazes para identificar irregularidades e promover as ações necessárias para garantir a proteção das informações sensíveis.

Esta política é revisada ao menos anualmente ou sempre que houver mudança relevante de risco, tecnologia ou regulamentação. Alterações são aprovadas pela administração e comunicadas aos públicos internos pertinentes.

6. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A presente política define os princípios, regras e controles destinados a proteger a confidencialidade, integridade e disponibilidade das informações sob responsabilidade da Austria Capital Gestão, incluindo dados de clientes, investidores, contrapartes e carteiras sob gestão, em meios físicos e eletrônicos. Aplica-se a sócios, administradores, colaboradores, funcionários e terceiros autorizados.

Diretrizes

A segurança da informação na Austria Capital Gestão de Recursos pauta-se nos seguintes princípios:

a) Princípio do menor privilégio e necessidade de saber para concessão de acessos;

b) Barreiras informacionais para prevenir conflitos de interesse;

c) Rastreabilidade (credenciais individuais e logs de atividade) para identificar detentores de informação;

d) Proporcionalidade dos controles ao porte, perfil de risco e complexidade operacional;

e) Conformidade regulatória, LGPD e autorregulação aplicável.

A Área de Risco e Compliance é responsável pela Segurança da Informação e Cibernética, cabendo-lhe:

a) propor e implementar controles;
b) coordenar testes periódicos;
c) gerir acessos e barreiras informacionais;
d) conduzir respostas a incidentes.

Procedimentos

O acesso a informações é concedido pelo princípio do menor privilégio, com credenciais individuais e registro de logs que possibilitem identificar usuários, ações e períodos. Em casos de alteração de função ou desligamento, os acessos são revisados e revogados de forma imediata. O detalhamento técnico desses procedimentos encontra-se no Manual de Segregação de Atividades e Confidencialidade.

Os recursos tecnológicos disponibilizados pela Austria Capital Gestão de Recursos destinam-se exclusivamente ao exercício das atividades profissionais e devem ser utilizados de forma ética, responsável e em conformidade com esta política.

Todos os sócios, administradores, colaboradores, funcionários e terceiros autorizados devem adotar as medidas necessárias para preservar a segurança, integridade e disponibilidade das informações corporativas e dos ativos de tecnologia da gestora.

A seguir, são estabelecidas as regras e orientações de uso aceitável, subdivididas por categoria de recurso tecnológico:

a) **Estações de trabalho e dispositivos corporativos:** Os computadores, notebooks, celulares e demais equipamentos fornecidos pela Austria Capital Gestão de Recursos são de uso exclusivamente profissional. É vedada a instalação de softwares, aplicativos ou extensões sem autorização da Área de Risco e Compliance. Os dispositivos devem possuir (i) bloqueio automático de tela após período de inatividade, para prevenir o acesso indevido; (ii) proteção antimalware e antivírus atualizada, aprovada e monitorada pela área de Risco e Compliance; (iii) sistema operacional e patches de segurança atualizados; (iv) O usuário é responsável por manter o equipamento sob sua guarda física em segurança, evitando exposição em locais públicos e assegurando que não seja utilizado por pessoas não autorizadas.
b) **Acesso remoto:** O acesso remoto aos sistemas e dados da Austria Capital Gestão de Recursos deve ocorrer apenas por meio de conexões seguras. É vedado o uso de redes Wi-Fi públicas ou desprotegidas (como as disponíveis em aeroportos, cafés, hotéis ou ambientes compartilhados) para acessar sistemas, arquivos ou e-mails corporativos, salvo se o dispositivo estiver conectado via VPN ativa e criptografada. Em qualquer cenário, é obrigação do colaborador verificar a legitimidade da rede, evitar o compartilhamento de senhas e assegurar o bloqueio automático do dispositivo em caso de inatividade. Essas medidas visam reduzir o risco de interceptação de dados, roubo de credenciais e infecção por softwares maliciosos durante conexões externas à rede corporativa. O acesso aos sistemas e informações corporativas deve ocorrer exclusivamente por meios autorizados, com autenticação multifator (MFA) ou single *sign-on* (SSO) para verificação de identidade. É proibida a sincronização automática de dados corporativos em dispositivos pessoais, contas de e-mail particulares ou mídias removíveis não autorizadas (ex.: pen drives, HDs externos, smartphones pessoais).
c) **E-mail corporativo e internet:** O e-mail corporativo deve ser utilizado exclusivamente para fins institucionais e nunca para assuntos pessoais. É proibido encaminhar mensagens ou arquivos contendo informações confidenciais para contas pessoais ou compartilhar dados da gestora em plataformas externas que não sejam autorizadas pela Área de Risco e Compliance. Todos devem manter atenção a mensagens suspeitas (phishing, engenharia social, falsos comunicados de fornecedores ou bancos). Em caso de dúvida, o colaborador deve evitar abrir links ou anexos e reportar imediatamente à

Área de Risco e Compliance. O acesso à internet deve ocorrer apenas para fins profissionais legítimos. É proibido visitar sites com conteúdo inapropriado, ilegal ou que possam representar risco à segurança da rede (downloads, streaming não autorizado, redes P2P, etc.).

d) **Mídias removíveis/serviços em nuvem pessoais:** É vedado o uso de mídias removíveis (como pen drives, HDs externos ou cartões de memória) para armazenar, copiar ou transferir informações da Austria Capital Gestão de Recursos, salvo quando expressamente autorizado pela Área de Risco e Compliance, mediante justificativa funcional e registro da autorização. Da mesma forma, é proibido utilizar serviços de nuvem pessoais para armazenar arquivos da gestora ou de clientes. O armazenamento de dados corporativos deve ser feito exclusivamente no ambiente Microsoft 365 corporativo dedicado da gestora, que oferece controle de acesso, criptografia e registro de atividades.

e) **Responsabilidade do usuário:** Cada usuário é responsável pela proteção e pelo uso adequado dos recursos tecnológicos sob sua responsabilidade. Qualquer incidente de segurança, suspeita de acesso indevido, perda, roubo de equipamento ou falha de sistema deve ser imediatamente comunicado à Área de Risco e Compliance, para que sejam adotadas as medidas cabíveis. O descumprimento das regras aqui previstas constitui violação às normas internas e poderá ensejar sanções disciplinares, sem prejuízo de eventuais responsabilidades legais ou regulatórias.

Contratações de provedores de tecnologia, nuvem ou serviços que processem dados da gestora deverão receber aprovação formal da Área de Risco e Compliance, que deverá garantir que tenha sido observado processo prévio de *due diligence* proporcional ao risco, contemplando a assinatura de Acordo de Confidencialidade (NDA), cláusulas contratuais de segurança da informação e proteção de dados, e controles de acesso segregado e monitorado

Austria Capital Gestão de Recursos mantém rotina de backup dos dados críticos em ambiente de nuvem Microsoft 365, dedicado e exclusivo da gestora, com procedimento de restauração testado pelo menos semestralmente.

Testes periódicos de segurança

A Austria Capital Gestão de Recursos adota mecanismos de monitoramento e testes periódicos de segurança com o objetivo de garantir a confidencialidade, integridade e disponibilidade das informações sob sua responsabilidade, mitigando riscos operacionais, tecnológicos e de vazamento de dados.

A Área de Risco e Compliance é responsável por planejar, executar e documentar os testes periódicos com a finalidade de identificar falhas ou potenciais fragilidades nos processos internos e coordenar as rotinas de controle e avaliação da infraestrutura tecnológica da gestora, podendo, quando necessário, contar com apoio de prestadores de serviços especializados.

Os testes e verificações seguem periodicidade e escopo proporcionais ao porte e à complexidade das operações da gestora, e compreendem, no mínimo:

a) Verificação semestral das permissões e acessos aos sistemas utilizados, assegurando que apenas usuários autorizados mantenham credenciais ativas, conforme o princípio do menor privilégio;

b) Revisão semestral de registros de acesso e de eventuais incidentes de segurança, com foco em atividades críticas;

c) Teste semestral de restauração de backups, a fim de validar a integridade e disponibilidade das informações;

d) Avaliação anual das condições de segurança tecnológica, incluindo atualização de softwares, revisão de políticas de senhas e verificação da proteção antivírus e firewall dos equipamentos corporativos.

O monitoramento contínuo contempla indicadores como disponibilidade e desempenho dos sistemas utilizados, incidentes de segurança reportados e comportamentos anômalos observados em dispositivos corporativos.

Eventuais achados, planos de ação e evidências dos testes são documentados e arquivados pela Área de Risco e Compliance, permanecendo disponíveis por, no mínimo, 5 (cinco) anos. Quando identificadas vulnerabilidades ou falhas de controle, são adotadas medidas corretivas imediatas e reavaliada a eficácia dos mecanismos implementados.

Controles de acesso

O controle de acesso às informações confidenciais é realizado com base em credenciais individuais, logs automáticos e autenticação multifator, o que permite identificar o detentor de cada informação e atribuir responsabilidades em caso de incidente.

A cada movimentação, alteração de função ou desligamento, os acessos são imediatamente revisados e, se necessário, revogados.

Plano de continuidade operacional

O plano de continuidade operacional considera as prioridades de negócio, a recuperação tempestiva de serviços essenciais e a comunicação adequada às partes impactadas, garantindo a preservação da integridade das informações e a retomada segura das atividades em caso de incidente.

Em caso de suspeita ou confirmação de incidente de segurança da informação — incluindo infecção por malware, acesso não autorizado, vazamento de dados, interrupção de serviços ou qualquer outro comprometimento da integridade, confidencialidade ou disponibilidade das informações —, a Área de Risco e Compliance deverá ser comunicada imediatamente.

A partir do registro do incidente, a Área de Risco e Compliance coordenará a resposta e as medidas de contingência, avaliando a natureza, a gravidade e o alcance do evento, bem como os sistemas, dados ou usuários potencialmente afetados.

A análise do incidente pela Área de Risco e Compliance compreenderá as seguintes etapas: (i) identificação das causas e origens do incidente; (ii) verificação de eventuais vulnerabilidades; (iii) determinação das responsabilidades envolvidas; e (iv) definição das etapas de recuperação e restauração dos sistemas ou dados impactados. Sempre que aplicável, serão adotadas medidas de mitigação imediata, como a suspensão temporária de acessos, o isolamento de sistemas comprometidos ou a atualização dos controles de segurança.

Concluída a análise preliminar, a Área de Risco e Compliance implementará o plano de ação de resposta e avaliará a necessidade de comunicação às partes internas e externas afetadas,

incluindo clientes, administradores fiduciários, provedores de tecnologia, órgãos reguladores e demais *stakeholders* relevantes, observando as obrigações legais e regulatórias aplicáveis.

O plano de ação de resposta a incidentes contempla: (i) contenção e isolamento, quando necessário; (ii) análise de causa e escopo; (iii) restauração segura de serviços e dados; (iv) definição de responsabilidades e medidas corretivas; (v) comunicações a clientes, administradores fiduciários e autoridades reguladoras, quando aplicável; e (vi) lições aprendidas, com ajustes nos controles internos e de segurança.

A Área de Risco e Compliance manterá registro completo do incidente e de todas as etapas do ciclo de resposta, assegurando a rastreabilidade e a documentação das ações adotadas.

A Área de Risco e Compliance é responsável por revisar esta política de forma periódica, no mínimo anualmente, e propor sua atualização sempre que houver mudanças relevantes de risco, tecnologia ou regulamentação.

Todos os integrantes participam de treinamento inicial e reciclagem anual ou por evento sobre confidencialidade, condutas vedadas, boas práticas de segurança, reporte de incidentes e engenharia social. Presenças e avaliações são registradas pela Área de Risco e Compliance.

7. PROGRAMA DE TREINAMENTOS

A Austria Capital Gestão de Recursos adota um programa de treinamento contínuo voltado a assegurar que todos os colaboradores atuem em conformidade com os princípios éticos, as normas internas e a regulamentação vigente.

Treinamento inicial

Todo novo colaborador participa, no momento da contratação, de um treinamento inicial conduzido pela área de Risco e Compliance, que tem por finalidade apresentar:

a) a estrutura organizacional e as principais atividades da gestora;

b) o Código de Ética e Conduta;

c) as políticas de controles internos, de confidencialidade e de segurança da informação;

d) as regras sobre prevenção a conflitos de interesse, negociações pessoais e condutas vedadas;

e) as responsabilidades individuais quanto ao cumprimento das normas regulatórias aplicáveis às atividades da gestora.

Durante o treinamento inicial, o colaborador tem oportunidade de esclarecer dúvidas e é formalmente cientificado de que o descumprimento das regras internas poderá ensejar medidas disciplinares.

Programa de reciclagem

A Austria Capital Gestão de Recursos promove reciclagens em frequência mínima anual ou sempre que houver atualizações relevantes nas normas internas ou na regulamentação aplicável. Esses treinamentos são conduzidos pela área de Risco e Compliance e têm como objetivo reforçar a cultura de controles internos, governança e ética, garantindo o alinhamento

permanente da equipe com os valores e as políticas da gestora. O conteúdo abrange, entre outros temas:

f) prevenção ao uso indevido de informação privilegiada (Insider Trading);

g) prevenção à lavagem de dinheiro e financiamento ao terrorismo;

h) conduta ética, prevenção ao assédio e à discriminação;

i) confidencialidade, proteção de dados pessoais (LGPD) e segurança da informação;

j) sustentabilidade e aspectos ESG aplicados à gestão de recursos.

A área de Risco e Compliance é responsável por coordenar o programa de treinamentos, acompanhar a participação dos colaboradores e manter registros atualizados das evidências e materiais utilizados, assegurando a rastreabilidade e a comprovação do cumprimento das obrigações junto aos órgãos reguladores.

Sempre que necessário, poderão ser realizados treinamentos complementares presenciais ou virtuais, conduzidos internamente ou por instrutores externos, de acordo com necessidades específicas da gestora, identificadas pela área de Risco e Compliance.

Todos os colaboradores são obrigados a participar dos treinamentos, registrando sua presença e ciência dos conteúdos apresentados. A área de Risco e Compliance é responsável por garantir que o programa de treinamentos contemple as políticas e procedimentos adotados pela gestora e seja sempre compatível com a atividade desempenhada pelo participante.

8. SEGREGAÇÃO DE ATIVIDADES

A Austria Capital Gestão de Recursos adota procedimentos de segregação de atividades com o objetivo de restringir o acesso a informações confidenciais e privilegiadas apenas a colaboradores cuja atuação funcional exija tal acesso, prevenindo vazamentos, conflitos de interesse e outras condutas vedadas pela legislação e regulamentação aplicável.

A área de Risco e Compliance é responsável por supervisionar a aplicação desses princípios e por propor ajustes sempre que necessário, em conformidade com a legislação vigente e as políticas internas da gestora.

A área de Risco e Compliance possui acesso irrestrito às informações eletrônicas disponíveis, em razão de suas funções institucionais de supervisão e monitoramento dos controles internos.

A separação eletrônica de informações e a aplicação de controles de acesso contribuem para garantir a integridade e a confidencialidade dos dados, além de mitigar o risco de conflitos de interesse, reforçando os pilares de governança e segurança da informação da gestora.

As regras e procedimentos detalhados sobre segregação física, funcional e sistêmica estão descritos no Manual de Segregação das Atividades e Confidencialidade da Austria Capital Gestão de Recursos, que complementa e operacionaliza as diretrizes deste Manual de Controles Internos e Compliance.

9. GESTÃO DE RISCOS E MANUTENÇÃO DE ARQUIVOS

A Austria Capital Gestão de Recursos adota práticas de gestão de riscos integradas às atividades de compliance, assegurando o monitoramento e a mitigação contínua de riscos operacionais, regulatórios, legais e reputacionais relacionados à sua atividade.

A gestora mantém arquivados em meio eletrônico todos os documentos e registros operacionais relevantes, em conformidade com os prazos e formatos exigidos pela regulamentação vigente, garantindo sua rastreabilidade e pronta disponibilização à CVM e demais órgãos competentes, quando solicitado.

As políticas internas e documentos institucionais de caráter público são revisados periodicamente, de modo a assegurar sua aderência às normas aplicáveis e a transparência perante clientes, investidores e demais partes interessadas.

A gestora mantém arquivados todos os documentos e registros operacionais relacionados à sua atividade, em conformidade com os prazos e formatos exigidos pela regulamentação vigente.

A área de Risco e Compliance é responsável por revisar e atualizar periodicamente todas as políticas internas da gestora, garantindo sua aderência às normas regulatórias e às melhores práticas de mercado.

Além disso, a área deverá verificar se os documentos institucionais de caráter público estão devidamente atualizados e disponíveis no site oficial da gestora, de forma clara, acessível e transparente para clientes, investidores e demais partes interessadas.

10.PLANO DE CONTINUIDADE DE NEGÓCIOS (PCN)

O Plano de Continuidade de Negócios (PCN) da Austria Capital Gestão de Recursos tem por finalidade assegurar a retomada das operações críticas e a preservação das informações e dos serviços prestados aos clientes em situações de contingência, falhas técnicas, interrupções de sistemas, indisponibilidade de infraestrutura ou outros eventos que possam comprometer a continuidade das atividades.

O PCN é estruturado de forma proporcional ao porte, à complexidade e ao volume operacional da Gestora, conforme previsto na Resolução CVM nº 21/2021 e nas melhores práticas de governança operacional.

Escopo e Abrangência

O PCN abrange todos os processos críticos da Austria Capital, incluindo:

a) Gestão e controle das carteiras de valores mobiliários sob administração;
b) Rotinas de backoffice e reconciliação de posições;
c) Monitoramento de risco e compliance;
d) Comunicação com clientes, contrapartes, custodiante e administradores fiduciários;
e) Segurança da informação e acesso aos sistemas corporativos.

Estrutura e Responsabilidades

a) Diretor de Risco e Compliance: Responsável por coordenar a implementação e o cumprimento do PCN, supervisionar os testes de contingência, aprovar revisões e documentar eventuais incidentes de continuidade.

b) Analista de Risco e Compliance: Responsável por executar os testes de restauração de dados, registrar evidências, monitorar incidentes e manter atualizadas as informações de contato e acesso remoto.
c) Diretor de Gestão: Responsável por assegurar a continuidade da gestão das carteiras e comunicação tempestiva com clientes e contrapartes em caso de indisponibilidade operacional.
d) Analista de Gestão: Responsável por manter atualizados os controles operacionais e garantir a integridade dos dados e planilhas utilizados nas rotinas diárias de investimento e controle.

Medidas de Continuidade

Em caso de interrupção das atividades, as seguintes medidas são adotadas:

a) Acesso remoto: todos os colaboradores possuem acesso seguro aos sistemas e arquivos corporativos por meio do ambiente Microsoft 365, com autenticação multifator (MFA) e backup automático em nuvem;
b) Backup e recuperação: os dados críticos são armazenados em ambiente de nuvem corporativo, com cópias de segurança automáticas e teste semestral de restauração;
c) Ambiente alternativo de trabalho: em caso de indisponibilidade física do escritório, o trabalho poderá ser conduzido integralmente em regime remoto, sem prejuízo das rotinas de gestão, controle e comunicação;
d) Comunicação e contingência: a comunicação com clientes, contrapartes e prestadores de serviço será priorizada via e-mail corporativo, telefone celular e Microsoft Teams;
e) Continuidade operacional mínima: as rotinas essenciais (execução de ordens, conciliações, monitoramento de risco e comunicação com clientes) serão priorizadas até a normalização completa dos sistemas e processos.

Testes e Revisões

a) O PCN é testado pelo menos uma vez por ano, preferencialmente mediante simulação de falha de acesso aos sistemas ou indisponibilidade temporária de infraestrutura;
b) A Área de Risco e Compliance é responsável por documentar os resultados, lições aprendidas e eventuais ajustes necessários;
c) O plano é revisado anualmente ou sempre que houver mudanças relevantes na estrutura tecnológica, no ambiente operacional ou nos prestadores de serviço críticos.

Registros e Evidências

a) Todos os testes, revisões e incidentes de continuidade são registrados e arquivados eletronicamente pela Área de Risco e Compliance, com guarda mínima de 5 (cinco) anos;
b) As evidências incluem data, escopo, participantes, resultados, medidas adotadas e eventuais ajustes realizados no plano;
c) Os registros permanecem à disposição da administração, da auditoria e dos órgãos de supervisão.

Comunicação e Encerramento de Incidentes

Em caso de incidente de continuidade relevante, o Diretor de Risco e Compliance:

a) Notificará imediatamente a Diretoria de Gestão;
b) Avaliará o impacto sobre as operações e a integridade das informações;

c) Coordenará as medidas corretivas e a comunicação aos clientes e contrapartes, quando aplicável;
d) Elaborará relato de encerramento do incidente, contendo a causa, impacto, tempo de recuperação e ações preventivas adotadas.

Disposições Finais

A Austria Capital Gestão de Recursos mantém o compromisso de garantir a continuidade de suas atividades e a proteção dos interesses de seus clientes, adotando práticas proporcionais e eficientes de contingência operacional e segurança da informação.

O PCN é parte integrante das políticas de Segurança da Informação e Gestão de Riscos, e reflete o compromisso da Gestora com a resiliência operacional e a conformidade regulatória.

11. VIGÊNCIA E ATUALIZAÇÃO

Esta Política tem vigência por prazo indeterminado e será revisada, no mínimo, anualmente ou sempre que houver necessidade de adequação regulatória ou aprimoramento de processos internos.

A versão vigente estará sempre disponível no site institucional da Austria Capital Gestão de Recursos, em conformidade com a regulamentação aplicável.