JPG GESTÃO DE RECURSOS LTDA

POLÍTICA INSTITUCIONAL

POLÍTICA DE CONTROLES INTERNOS, SEGREGAÇÃO DE ATIVIDADES E GESTÃO DE RISCOS

DATA DE CRIAÇÃO
15/10/2025

CONTEÚDO DESTE DOCUMENTO

1. OBJETIVO

A presente Política tem como objetivo estabelecer as regras, procedimentos e descrição dos controles internos, além da Gestão de Risco da JPG GESTÃO DE RECURSOS LTDA, em conformidade com o disposto nos artigos 22 e 23, incisos I e II, da Resolução CVM nº 21/2021.

Os controles internos são fundamentais para a sustentabilidade do negócio de gestão de recursos, pois asseguram a integridade das operações, protegem os interesses dos investidores e mantêm a reputação da instituição no mercado. Sem controles adequados, a empresa fica exposta a riscos operacionais, regulamentares e reputacionais que podem comprometer sua continuidade.

Este documento visa assegurar o permanente atendimento às normas, políticas e regulamentações vigentes, referentes à atividade de gestão de carteiras de valores mobiliários (não incluindo administração fiduciária nem distribuição de valores mobiliários).

2. APLICAÇÃO

Esta política aplica-se a todos os sócios e administradores da JPG GESTÃO DE RECURSOS LTDA, funcionários e colaboradores, prestadores de serviços terceirizados e todas as atividades relacionadas à gestão de carteiras.

3. REGULAMENTAÇÃO ASSOCIADA

- **Resolução CVM nº 21/2021**: Esta é a norma principal que regula a atividade de gestão de carteiras no Brasil, estabelecendo requisitos para registro, funcionamento e controles internos.
- **Resolução CVM nº 50/2021**: Define obrigações específicas para o setor de valores mobiliários em relação à prevenção da lavagem de dinheiro e financiamento ao terrorismo.

4. GLOSSÁRIO

- **Gestão de Carteiras**: Gestão profissional de recursos de terceiros em valores mobiliários.
- **Controles Internos:** Conjunto de procedimentos e políticas estabelecidos para assegurar o cumprimento de objetivos operacionais e regulamentares.
- **Informações Privilegiadas:** Informações relevantes sobre valores mobiliários que não tenham sido divulgadas ao mercado.
- **Segregação de Funções:** Separação de responsabilidades para evitar conflitos de interesse e erros.
- **Alta Administração:** Diretor de Gestão de Recursos e Diretor de Riscos, Compliance e PLD-FTP

5. ESTRUTURA DE GOVERNANÇA

A governança corporativa na gestão de carteiras requer estrutura específica que garanta supervisão adequada dos controles internos e tomada de decisão transparente. A JPG GESTÃO DE RECURSOS LTDA estabelece uma estrutura de governança robusta e adequada ao seu porte e complexidade.

5.1. Comitê de Controles Internos

O Comitê de Controles Internos representa o órgão máximo de supervisão dos controles internos da JPG GESTÃO DE RECURSOS LTDA, sendo responsável pela definição de diretrizes, aprovação de políticas e monitoramento da efetividade dos controles implementados.

5.1.1. Composição:

- Diretor Presidente, Diretor de Compliance e Diretor de Riscos.

5.1.2. Responsabilidades:

- **Aprovar políticas e procedimentos**: Todas as políticas de controles internos devem ser formalmente aprovadas pelo Comitê de Controles Internos, garantindo alinhamento com a estratégia da empresa, como: aprovação anual da política de controles internos, aprovação de mudanças em limites de risco, aprovação de novos procedimentos operacionais.
- **Monitorar efetividade dos controles:** O Comitê deve receber relatórios regulares sobre o funcionamento dos controles e tomar ações corretivas quando necessário, tal como: análise mensal de indicadores de controle e acompanhamento de planos de ação corretivos.
- **Avaliar incidentes e não conformidades:** Todos os incidentes relevantes devem ser reportados ao Comitê para avaliação e definição de ações corretivas, por exemplo: investigação de violações de limites, análise de falhas operacionais, avaliação de reclamações de clientes, revisão de perdas operacionais.
- **Definir planos de ação corretivos:** O Comitê deve definir e acompanhar a implementação de ações corretivas para deficiências identificadas, como cronograma de implementação de melhorias, definição de responsáveis por ações corretivas, acompanhamento de prazos, avaliação de efetividade das correções.

5.2. Linhas de Defesa

O modelo de três linhas de defesa é amplamente reconhecido como best practice em gestão de riscos e controles internos, proporcionando camadas independentes de verificação e controle.

5.2.1. Primeira Linha: Áreas operacionais.

As áreas operacionais são proprietárias dos riscos e responsáveis pela implementação e execução dos controles primários, representam a primeira barreira contra riscos e devem ter controles incorporados aos processos operacionais.

- **Execução das atividades:** Gestores de carteira devem executar estratégias de investimento conforme mandatos aprovados, operadores devem executar ordens dentro de limites estabelecidos, analistas devem seguir metodologias padronizadas de análise.
- **Controles primários:** é obrigatório a verificação de limites antes da execução de operações, conferência de dados antes de envio de relatórios, validação de preços de mercado e verificação de documentação de clientes.
- **Automonitoramento:** Implementação de relatórios diários de posições e exposições, acompanhamento de performance versus benchmark, monitoramento de liquidez das carteiras, verificação de aderência a mandatos.

5.2.2. Segunda Linha: Compliance

Monitorar e avaliar a efetividade dos controles da primeira linha, proporcionando supervisão e orientação, fornecendo visão independente sobre adequação dos controles e aderência a políticas e regulamentações.

- **Monitoramento independente:** Verificação de aderência a limites de risco, monitoramento de operações suspeitas para PLD/FT, verificação de conflitos de interesse.
- **Avaliação de controles:** Testes periódicos de controles operacionais, avaliação de adequação de políticas, revisão de procedimentos, análise de efetividade de treinamentos.
- **Orientação e suporte**: Treinamentos sobre mudanças regulamentares, orientação sobre interpretação de normas, suporte na implementação de novos controles, esclarecimentos sobre políticas internas.

5.2.3. Terceira Linha: Gestão de Riscos

Função que avalia a adequação e efetividade do sistema completo de controles internos. Proporciona asseguração independente sobre a efetividade da governança, gestão e controles internos.

- **Avaliação Anual:** Avaliação anual dos controles de investimento, revisão da efetividade dos controles de PLD/FT, avaliação da adequação da estrutura de governança, teste de controles de TI.
- **Testes de efetividade:** Teste de operacionalidade de controles automáticos, verificação de aderência a procedimentos documentados, teste de efetividade de segregação de funções, avaliação de controles de acesso.
- **Recomendações de melhoria:** Sugestões de automação de controles manuais, recomendações de melhorias em políticas, propostas de otimização de processos, identificação de gaps de controle

6. CONTROLES INTERNOS FUNDAMENTAIS

Os controles internos fundamentais representam os pilares sobre os quais toda a estrutura de controles da JPG GESTÃO DE RECURSOS LTDA está construída. Estes princípios devem estar presentes em todos os processos e atividades da empresa.

6.1. PRINCÍPIOS BÁSICOS

Os princípios básicos de controles internos são universalmente reconhecidos como elementos essenciais para uma estrutura de controles efetiva. Sua aplicação reduz significativamente os riscos operacionais e regulamentares.

6.1.1. Segregação de Funções

Segregação de funções é um dos controles mais importantes na JPG GESTÃO DE RECURSOS LTDA, evitando que uma única pessoa tenha controle completo sobre uma transação do início ao fim. Ela reduz drasticamente o risco de fraude e erros, além de criar verificações naturais nos processos.

6.1.2. Separação entre execução e controle

O analista que recomenda um investimento não pode ser o mesmo que executa a operação; a pessoa que registra uma operação não pode ser a mesma que a aprova; quem elabora relatórios não pode ser quem os aprova para envio aos clientes.

6.1.3. Aprovação por pessoa diferente do executor

Operações acima de determinado valor devem ser aprovadas por supervisor; pagamentos devem ser autorizados por pessoa diferente de quem os prepara; abertura de contas de clientes deve ser aprovada por compliance.

6.1.4. Revisão das operações

Back office revisa todas as operações executadas pelo front office; compliance revisa periodicamente as decisões de investimento; a gestão de riscos testa a efetividade dos controles implementados.

6.1.5. Alçadas de Aprovação

Limites de autoridade que garante que decisões sejam tomadas no nível hierárquico apropriado, considerando seu impacto e risco. Isso evita que decisões críticas sejam tomadas por pessoas sem autoridade adequada e garante que Alta Administração esteja envolvida em decisões relevantes.

6.1.6. Limites por função e valor

Analistas júnior podem recomendar investimentos até R$ 1 milhão; analistas sênior até R$ 5 milhões; gestores até R$ 20 milhões; acima disso requer aprovação do comitê de investimento. Operadores podem executar ordens até determinado valor sem aprovação adicional.

6.1.7. Aprovação em múltiplos níveis

Investimentos em novos setores, abertura de contas para PEPs e contratação de prestadores de serviços críticos, requerem aprovação da Alta Administração.

6.1.8. Documentação das decisões

Atas de reuniões de comitê de investimento com justificativas para decisões; e-mails de aprovação com reasoning para investimentos específicos; formulários padronizados de aprovação com campos obrigatórios preenchidos.

6.1.9. Registros e Documentação

Manutenção adequada de registros é fundamental para rastreabilidade, auditoria e cumprimento de obrigações regulamentares, permitindo a reconstrução de decisões e transações, facilitando auditorias e investigações, e garante cumprimento de prazos regulamentares de retenção.

6.1.10. Manutenção de registros completos

Registro de todas as ordens de investimento com data, hora, responsável e justificativa; manutenção de gravações de conversas telefônicas relevantes; arquivo de todos os relatórios enviados aos clientes; registro de todas as reuniões de comitê.

6.1.11. Rastreabilidade das operações

Cada operação deve ter um número único de identificação; sistema deve registrar quem inseriu, quem aprovou e quem executou cada operação; alterações em dados devem manter histórico de versões anteriores.

6.1.12. Arquivo por prazo regulamentar

Documentos de PLD/FT devem ser mentidos por 10 anos; registros de operações e correspondências com clientes devem ser mantidos por, no mínimo, 10 anos.

7. POLÍTICA DE CONFIDENCIALIDADE

A confidencialidade é um pilar fundamental para a JPG GESTÃO DE RECURSOS LTDA. O acesso a informações privilegiadas pode ser constante e o vazamento pode causar danos irreparáveis tanto aos nossos clientes investidores.

7.1. REGRAS DE SIGILO E CONDUTA

A Instrução CVM 358/2002 e a Resolução CVM 21/2021 estabelecem obrigações rigorosas quanto ao tratamento de informações privilegiadas e confidenciais, sendo o descumprimento passível de penalidades severas. A presente política abrange todos os indivíduos que tenham acesso a informações sensíveis, independentemente de sua relação formal com a JPG GESTÃO DE RECURSOS LTDA.

7.1.1. Sócios, administradores, colaboradores e funcionários

Pessoas internas que têm acesso mais amplo a informações confidenciais e devem ser os primeiros a dar exemplo de conduta adequada. São obrigações: não comentar sobre posições das carteiras em ambientes sociais; não

utilizar informações sobre investimentos para benefício próprio; não compartilhar análises internas com pessoas não autorizadas; manter sigilo sobre estratégias de investimento.

7.1.2. Prestadores de serviços terceirizados

Terceiros que podem ter acesso a informações confidenciais no curso de seus serviços e devem estar sujeitos às mesmas obrigações de sigilo, como por exemplo: auditores que acessam informações sobre carteiras; prestadores de serviços de TI que têm acesso a sistemas; consultores que participam de discussões estratégicas; advogados que assessoram em operações específicas.

7.1.3. Todas as informações confidenciais

Esta política cobre todas as categorias de informações confidenciais, não apenas informações privilegiadas no sentido regulamentar. Informações sobre performance das carteiras; dados pessoais e financeiros dos clientes; estratégias de investimento; informações sobre due diligence de investimentos; dados sobre rentabilidade da gestora.

7.1.4. Exigências:

Para garantir efetividade da política de confidencialidade, a JPG GESTÃO DE RECURSOS LTDA exige controles específicos e formalizações adequadas, tais como:

1. **Termo de confidencialidade assinado:** Formaliza as obrigações de sigilo e cria base legal para eventuais ações em caso de violação. Termo específico para funcionários com cláusulas sobre informações privilegiadas; termo para terceiros com definição clara de informações cobertas; termo para estagiários com linguagem adequada ao nível de responsabilidade; renovação periódica dos termos.
2. **Treinamento sobre sigilo:** Garante que todos compreendam suas obrigações e as consequências de violações. São exemplos: treinamento inicial obrigatório sobre política de confidencialidade; reciclagem anual com casos práticos; treinamento específico sobre mudanças regulamentares; simulações de situações de conflito.
3. **Monitoramento de acesso às informações:** Permite identificar acessos inadequados e investigar possíveis vazamento, tal como: Log de acesso a sistemas sensíveis; controle de impressão de documentos confidenciais; monitoramento de e-mails com informações sensíveis; auditoria periódica de acessos.

7.2. DETENTORES DE INFORMAÇÕES PRIVILEGIADAS

A Instrução CVM 358/2002 exige identificação e controle rigoroso de pessoas que tenham acesso a informações privilegiadas, sendo obrigatória a manutenção de lista atualizada.

7.2.1. Identificação

A identificação precisa de detentores de informações privilegiadas é fundamental para aplicação adequada de controles específicos e para investigação de eventuais vazamentos.

7.2.2. Lista atualizada de pessoas com acesso

Permite aplicação de controles específicos e facilita investigações em caso de vazamentos, tal como: lista com gestores de carteira que têm acesso a informações sobre investimentos específicos; analistas que participam de due diligence de empresas; membros de comitê de investimento que discutem estratégias; assistentes que têm acesso a documentos confidenciais.

7.2.3. Classificação por cargo e atribuição

Permite aplicação de controles diferenciados conforme o nível de acesso e responsabilidade, como: classificação em níveis (alto, médio, baixo acesso); identificação de pessoas com acesso a informações sobre empresas específicas; mapeamento de acesso por tipo de informação (mercado, crédito, estratégia); identificação de pessoas com acesso temporário.

7.2.4. Revisão trimestral da lista

Garante que a lista reflita a realidade atual e que controles sejam aplicados adequadamente. São ações obrigatórias: revisão após mudanças organizacionais; atualização quando pessoas mudam de função; inclusão de novos funcionários; exclusão de pessoas que deixaram a empresa; revisão de níveis de acesso.

7.2.5. Barreiras de Informação:

As barreiras de informação são controles físicos e lógicos que impedem o fluxo inadequado de informações privilegiadas entre áreas ou pessoas.

7.2.6. Segregação física de áreas sensíveis

Impede acesso casual a informações confidenciais e reduz riscos de vazamentos não intencionais, tal como: área de gestão separada fisicamente de outras áreas; salas de reunião com isolamento acústico; áreas restritas para discussão de investimentos sensíveis.

7.2.7. Controles de acesso a sistemas

Garante que apenas pessoas autorizadas tenham acesso a informações específicas nos sistemas, como: senhas individuais para cada usuário; perfis de acesso diferenciados por função; dupla autenticação para sistemas críticos; log de todas as atividades nos sistemas; desativação automática de acessos inativos.

7.2.8. Restrições de comunicação

Evita vazamentos através de comunicações inadequadas entre áreas ou com terceiros, tais como: política de uso de e-mail para informações confidenciais; restrições para discussão de investimentos em áreas comuns; controles para comunicação com imprensa; procedimentos para comunicação com investidores.

7.3. CONTROLES DE ACESSO

Em um ambiente cada vez mais digital, A JPG GESTÃO DE RECURSOS LTDA acredita que os controles de acesso tecnológicos são fundamentais para proteção de informações confidenciais.

São ações obrigatórias na JPG GESTÃO DE RECURSOS LTDA:

7.3.1. Sistemas de Informação:

Os sistemas de informação concentram grande volume de informações confidenciais e requerem controles rigorosos de acesso.

7.3.2. Senhas individuais e intransferíveis

Garante rastreabilidade de ações nos sistemas e responsabilização individual. Por exemplo: política de senhas complexas com renovação periódica; proibição de compartilhamento de senhas; senhas diferentes para sistemas diferentes; bloqueio automático após tentativas incorretas.

7.3.3. Arquivo seguro para informações sensíveis

Protege documentos críticos contra acesso não autorizado, danos ou perda, como cofre para documentos críticos; sala com acesso controlado; backup físico de documentos eletrônicos críticos.

7.3.4. Destruição segura de documentos

Evita que informações confidenciais sejam recuperadas após descarte inadequado, como fragmentadora de alta segurança para documentos confidenciais; procedimento formal para destruição com testemunhas; certificado de destruição para documentos críticos; cronograma de destruição conforme prazos regulamentares.

8. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é crítica para a gestão de carteiras, onde falhas podem resultar em perdas financeiras significativas, violações regulamentares e danos reputacionais irreversíveis. A JPG GESTÃO DE RECURSOS LTDA implementa controles robustos para proteger todas as informações sob sua responsabilidade.

8.1. TESTES PERIÓDICOS DE SEGURANÇA

Em um ambiente de constante evolução das ameaças cibernéticas, testes regulares de segurança são essenciais para identificar vulnerabilidades antes que sejam exploradas por agentes maliciosos.

São testes implementados na JPG GESTÃO DE RECURSOS LTDA:

8.1.1. Sistemas Eletrônicos:

Os sistemas eletrônicos da JPG GESTÃO DE RECURSOS LTDA processam informações altamente sensíveis e movimentam recursos significativos, sendo alvos atrativos para ataques cibernéticos. Realizamos testes proativos que identificam a vulnerabilidades antes que sejam exploradas, reduzindo significativamente o risco de incidentes de segurança.

8.1.2. Avaliação de vulnerabilidades

Scan automatizado mensal de todos os sistemas em busca de vulnerabilidades conhecidas; análise de configurações de segurança de servidores e workstations; verificação de atualizações de segurança pendentes; avaliação de força de senhas utilizadas nos sistemas; teste de efetividade de controles de acesso.

8.1.3. Atualização de sistemas de segurança

Atualização mensal de antivírus e anti-malware; aplicação de patches de segurança em prazo máximo de 30 dias; atualização de firewalls com novas regras de proteção; renovação anual de certificados digitais; upgrade de sistemas de detecção de intrusão.

8.1.4. Periodicidade:

A definição de periodicidades adequadas para testes de segurança equilibra a necessidade de proteção com a eficiência operacional. Periodicidades bem definidas garantem cobertura adequada sem sobrecarregar as operações.

1. **Testes mensais de backup:** Restauração completa de um sistema a partir do backup para verificar integridade; teste de recuperação de dados específicos de carteiras; verificação de tempo de recuperação (RTO) versus objetivos estabelecidos; teste de backup incremental e diferencial; validação de backup de configurações de sistemas críticos.

2. **Avaliação trimestral de controles:** Revisão de logs de acesso aos sistemas críticos; verificação de efetividade de controles de segregação de funções; teste de controles automáticos de limites; avaliação de aderência a políticas de senha; revisão de permissões de usuários nos sistemas.
3. **Revisão anual da política:** Atualização da política conforme mudanças tecnológicas; incorporação de lições aprendidas de incidentes; alinhamento com novas regulamentações; aprovação formal pela Alta Administração.

8.2. IDENTIFICAÇÃO E RESPONSABILIZAÇÃO

A capacidade de identificar usuários e rastrear suas ações é fundamental tanto para fins de controle interno quanto para atendimento a requisitos regulamentares e investigações.

8.2.1. Rastreabilidade

Em caso de incidentes ou investigações, a capacidade de rastrear ações específicas a usuários individuais é crítica para identificar causas e responsabilidades. Permite investigações efetivas e cria incentivos para comportamento adequado dos usuários.

1. **Log detalhado de acesso:** Registro de data, hora, usuário e ação para cada acesso aos sistemas de gestão; log de consultas específicas realizadas em bases de dados de clientes; registro de modificações em carteiras com identificação do responsável; log de impressões de documentos confidenciais; registro de acessos remotos com localização geográfica.
2. **Identificação única de usuários:** Cada funcionário possui login único e intransferível; contas de serviço identificadas e controladas; proibição de contas compartilhadas;
3. **Monitoramento de atividades suspeitas:** Alertas automáticos para acessos fora do horário comercial; notificação de tentativas de acesso a informações não relacionadas à função do usuário; monitoramento de downloads massivos de informações; detecção de padrões anômalos de acesso; alertas para múltiplas tentativas de login incorretas.

8.2.2. Responsabilização

A responsabilização efetiva por violações de segurança é essencial para manter a cultura de segurança e desencorajar comportamentos inadequados. Demonstra seriedade da organização em relação à segurança e cria consequências reais para violações.

1. **Investigação de vazamentos:** Procedimento formal para investigação de suspeitas de vazamento de informações privilegiadas; análise de sistemas em caso de incidentes; entrevistas com pessoas com acesso às informações vazadas; análise de comunicações eletrônicas quando autorizado; relatório formal de investigação com conclusões e recomendações.
2. **Medidas disciplinares:** Advertência verbal para violações leves e não recorrentes; Advertência escrita para violações moderadas ou recorrentes; Suspensão temporária para violações graves; Demissão por justa causa para violações muito graves ou recorrentes após advertências. A aplicação de medidas disciplinares deve observar: Direito de defesa do acusado; Proporcionalidade entre a violação e a sanção; Análise de circunstâncias atenuantes e agravantes; Documentação completa do processo; Aprovação pela Alta Administração.
3. **Comunicação às autoridades quando necessário:** Comunicação à CVM em caso de vazamento de informações privilegiadas; notificação à Polícia Federal em caso de crimes cibernéticos; comunicação ao COAF para operações suspeitas relacionadas a segurança; notificação a clientes em caso de vazamento de dados pessoais; comunicação a órgãos de proteção de dados quando aplicável.

8.3. PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (LGPD) e regulamentações específicas do mercado de capitais estabelecem obrigações rigorosas para proteção de dados pessoais e informações confidenciais.

8.3.1. Criptografia

A criptografia é a principal linha de defesa para proteger informações confidenciais contra acesso não autorizado, tanto durante transmissão quanto armazenamento. Mesmo em caso de violação de outros controles, dados criptografados permanecem protegidos contra acesso não autorizado.

1. **Dados em trânsito e em repouso:** Criptografia SSL/TLS para todas as comunicações via internet; criptografia de e-mails contendo informações confidenciais; criptografia de bases de dados com informações de clientes; criptografia de backups armazenados; comunicação criptografada com custodiantes e prestadores de serviços.
2. **Chaves de criptografia seguras:** Geração de chaves utilizando geradores de números aleatórios certificados; armazenamento de chaves em hardware security modules (HSM); rotação periódica de chaves conforme política estabelecida; segregação de chaves entre ambientes de produção e desenvolvimento; backup seguro de chaves em local separado.
3. **Atualização regular de algoritmos:** Migração de algoritmos obsoletos (como MD5) para algoritmos seguros (SHA-256); atualização de protocolos de criptografia conforme recomendações de segurança; monitoramento de vulnerabilidades em algoritmos utilizados; planejamento de migração para criptografia pós-quântica; testes regulares de força da criptografia implementada.

8.3.2. Backup e Recuperação:

A capacidade de recuperar informações e sistemas após incidentes é crítica para a continuidade dos negócios e cumprimento de obrigações fiduciárias, garantindo que a JPG GESTÃO DE RECURSOS LTDA possa continuar operando mesmo após incidentes significativos, protegendo os interesses dos investidores.

1. **Backup diário automatizado:** Backup automático de todas as bases de dados de carteiras ao final de cada dia útil; backup incremental durante o dia para capturar alterações críticas; backup de configurações de sistemas e aplicações; backup de logs de auditoria e controles; verificação automática de integridade dos backups realizados.
2. **Testes de recuperação mensais:** Restauração completa de um ambiente de teste a partir do backup; teste de recuperação de carteiras específicas; simulação de recuperação após desastre completo; teste de tempo de recuperação (RTO) e ponto de recuperação (RPO); documentação de lições aprendidas dos testes.
3. **Plano de continuidade de negócios:** Procedimentos detalhados para operação em local alternativo; lista de contatos críticos para acionamento em emergências; acordo com prestadores de serviços para suporte em contingências; treinamento regular da equipe em procedimentos de contingência; teste anual completo do plano de continuidade.

9. PROGRAMA DE TREINAMENTO

O programa de treinamento é fundamental para garantir que todos os envolvidos nas atividades da JPG GESTÃO DE RECURSOS LTDA compreendam suas responsabilidades e estejam capacitados para executar adequadamente os controles internos estabelecidos.

9.1. PÚBLICO-ALVO

A Resolução CVM 21/2021 exige que gestores de carteira mantenham programa de treinamento adequado para todos os funcionários envolvidos nas atividades regulamentadas.

9.1.1. Gestores e Funcionários:

O treinamento deve ser direcionado especificamente para as funções e responsabilidades de cada indivíduo, garantindo relevância e efetividade. Funcionários bem treinados são a primeira linha de defesa contra riscos operacionais e regulamentares.

1. **Quem acessa informações confidenciais deve seguir:** Treinamento específico sobre política de confidencialidade para analistas de investimento; capacitação sobre tratamento de informações privilegiadas para assistentes administrativos; treinamento sobre LGPD para funcionários que acessam dados pessoais de clientes; capacitação sobre controles de acesso para equipe de TI.
2. **Quem participa do processo de decisão de investimento deve seguir:** Treinamento sobre análise de risco para gestores de carteira; capacitação sobre due diligence para analistas de investimento; treinamento sobre limites regulamentares para operadores; capacitação sobre conflitos de interesse para membros de comitê de investimento.

9.2. CONTEÚDO

O conteúdo do treinamento é abrangente, atualizado e adequado às necessidades específicas de cada função. Conteúdo relevante e bem estruturado garante melhor absorção e aplicação prática dos conhecimentos.

9.2.1. Políticas e Procedimentos:

Todos os funcionários devem conhecer profundamente as políticas e procedimentos aplicáveis às suas funções.

1. Código de Ética
2. Política de Controles Internos, Segregação de Atividades e Gestão de Riscos
3. Prevenção à Lavagem de Dinheiro - PLD_FTP
4. Manual de Segregação de Atividades
5. Política de Compra, Venda, Rateio e Divisão de Ordens de Valores Mobiliários
6. Regulamentação CVM: Análise detalhada da Resolução CVM 21/2021 e suas implicações práticas

9.2.2. Compatibilidade:

O treinamento é específico para as atividades desempenhadas por cada funcionário, evitando conteúdo genérico demais ou específico demais. Treinamento compatível com as funções garante maior relevância e aplicabilidade prática.

1. **Treinamento específico por função:** Gestores de carteira recebem treinamento avançado sobre análise de risco; operadores são treinados especificamente em procedimentos de execução; equipe de compliance recebe capacitação sobre monitoramento e investigação; back office é treinado em procedimentos de reconciliação e controles.
2. **Conteúdo adequado às responsabilidades:** Funcionários com acesso a informações privilegiadas recebem treinamento específico sobre insider trading; equipe de TI recebe capacitação sobre segurança da informação; terceirizados são treinados conforme serviços prestados.
3. **Atualização conforme mudanças regulamentares:** Treinamento específico quando há mudanças na regulamentação CVM; capacitação sobre novas tipologias de PLD/FT; atualização sobre alterações na LGPD; treinamento sobre novas práticas de mercado; capacitação sobre novos produtos ou estratégias.

10. CONTROLES OPERACIONAIS

Os controles operacionais são a espinha dorsal da gestão de carteiras, garantindo que todas as operações sejam executadas de forma precisa, tempestiva e em conformidade com as políticas estabelecidas e mandatos dos

clientes.

10.1.GESTÃO DE CARTEIRAS

A gestão de carteiras envolve responsabilidade fiduciária, onde a JPG GESTÃO DE RECURSOS LTDA atua em nome e por conta dos investidores, exigindo controles rigorosos para proteger seus interesses.

10.1.1. Processo de Investimento

O processo de investimento deve ser estruturado e controlado para garantir que decisões sejam tomadas de forma consistente e adequada aos objetivos dos investidores. Por isso a JPG GESTÃO DE RECURSOS LTDA utiliza controles adequados no processo de investimentom protegendo tanto os investidores quanto a gestora de decisões inadequadas ou não autorizadas.

1. **Análise prévia de investimentos:** Relatório padronizado de análise para cada novo investimento com métricas de risco-retorno; due diligence obrigatória para investimentos acima de determinado valor; análise de adequação ao perfil da carteira antes da execução; verificação de disponibilidade de caixa antes de ordens de compra; análise de impacto no risco total da carteira.
2. **Aprovação conforme alçadas:** Investimentos até R$ 1 milhão aprovados por gestor sênior; investimentos entre R$ 1-5 milhões aprovados por diretor; investimentos acima de R$ 5 milhões aprovados pela Alta Administração; investimentos em novos setores sempre aprovados pela Alta Administração independentemente do valor; aprovação documentada com justificativa por escrito.
3. **Execução por pessoa autorizada:** Apenas operadores certificados podem executar ordens; sistema de dupla confirmação para operações acima de determinado valor; gravação de todas as ordens telefônicas; confirmação por escrito de ordens complexas; verificação de identidade para ordens por telefone.
4. **Confirmação independente:** Back office confirma todas as operações executadas pelo front office; reconciliação diária entre ordens dadas e operações executadas; confirmação de preços com fontes independentes; verificação de settlement de operações; confirmação de recebimento de títulos pelo custodiante.

10.1.2. Monitoramento de Limites

O monitoramento de limites é essencial para garantir que as carteiras permaneçam dentro dos parâmetros de risco estabelecidos e em conformidade com regulamentações. Evita exposições excessivas e garante conformidade com mandatos dos clientes e regulamentações aplicáveis.

1. **Limites por carteira e ativo:** Limite máximo de 5% por emissor privado em carteiras conservadoras; limite de 20% em ações para carteiras de renda fixa; limite de concentração setorial de 25%; limite de liquidez mínima de 10% em cada carteira; limite de exposição cambial conforme perfil do investidor.
2. **Aprovação para ultrapassagem:** Ultrapassagem temporária de limites aprovada por diretor com prazo para regularização; aprovação pela Alta Administração para mudanças permanentes em limites; documentação formal de justificativas para exceções; comunicação obrigatória ao cliente em caso de violação de mandato.

10.2.RECONCILIAÇÃO

A reconciliação é um controle fundamental que garante a integridade e precisão das informações financeiras e posições das carteiras. Identifica discrepâncias rapidamente, permitindo correções tempestivas e mantendo a confiabilidade das informações.

10.2.1. Posições

A reconciliação de posições garante que os registros internos estejam alinhados com os registros do custodiante, evitando discrepâncias que podem impactar decisões de investimento.

1. **Reconciliação diária com custodiante:** Comparação automática diária entre posições no sistema interno e extratos do custodiante; reconciliação de quantidade e valor de mercado de cada título; verificação de movimentações do dia (compras, vendas, juros, dividendos); reconciliação de posições em derivativos e suas garantias.
2. **Investigação de diferenças:** Procedimento formal para investigação de discrepâncias acima de R$ 1.000; análise de timing differences versus diferenças reais; verificação de operações em trânsito não refletidas; investigação de diferenças de preços com fontes múltiplas; documentação de todas as investigações realizadas.
3. **Ajustes tempestivos:** Correção de diferenças identificadas no mesmo dia quando possível; comunicação imediata ao custodiante para correção de erros; ajustes contábeis formais para diferenças confirmadas; processo de aprovação para ajustes acima de determinado valor.
4. **Documentação de exceções:** Registro formal de todas as diferenças identificadas e suas causas; arquivo de comunicações com custodiante sobre discrepâncias; documentação de ajustes realizados com aprovações necessárias; relatório mensal de exceções para a Alta Administração.

10.2.2. Movimentação Financeira

O controle da movimentação financeira é crítico para evitar fraudes e garantir que todos os pagamentos e recebimentos sejam adequadamente autorizados e registrados.

1. **Conciliação bancária diária:** Comparação diária entre saldo contábil e saldo bancário de todas as contas; identificação de lançamentos em trânsito e pendências; verificação de todas as movimentações do dia; reconciliação de aplicações financeiras e resgates.
2. **Conferência de transferências:** Verificação de dados bancários antes de cada transferência; confirmação de valores e finalidade de transferências; dupla conferência para transferências acima de determinado valor; confirmação de recebimento para transferências críticas.
3. **Aprovação de pagamentos:** aprovação do diretor para pagamentos acima de R$ 100.000; verificação de documentação suporte antes da aprovação; confirmação de adequação orçamentária para despesas.
4. **Arquivo de comprovantes:** Arquivo digital de todos os comprovantes de transferência; backup físico de comprovantes críticos; organização cronológica de documentos; retenção conforme prazos regulamentares estabelecidos.

11. CONTROLES DE RISCO

O gerenciamento de risco é fundamental na gestão de carteiras, protegendo os investidores contra perdas excessivas e garantindo que os riscos assumidos sejam adequados aos objetivos e perfil de cada carteira.

11.1.IDENTIFICAÇÃO DE RISCOS

A identificação adequada de riscos é o primeiro passo para um gerenciamento efetivo, permitindo que controles apropriados sejam implementados para cada tipo de exposição. Riscos não identificados não podem ser gerenciados, podendo resultar em perdas inesperadas e significativas para os investidores.

11.1.1. Tipos de Risco:

A gestão de carteiras está exposta a diversos tipos de risco que devem ser identificados, mensurados e controlados adequadamente.

1. **Risco de mercado:** Risco de variação de preços de ações devido a movimentos do mercado; risco de taxa

de juros em carteiras de renda fixa; risco cambial em investimentos denominados em moeda estrangeira; risco de volatilidade em posições de opções; risco de spread de crédito em debêntures corporativas.

2. **Risco de crédito:** Risco de default de emissor de debênture corporativa; risco de rebaixamento de rating de título público; risco de deterioração da qualidade creditícia de contraparte em derivativos; risco de concentração em poucos emissores; risco país para investimentos internacionais.
3. **Risco de liquidez:** Risco de não conseguir vender posições rapidamente sem impacto significativo no preço; risco de descasamento entre necessidade de caixa e liquidez dos ativos; risco de mercado secundário limitado para títulos específicos; risco de liquidez em períodos de stress do mercado.
4. **Risco operacional:** Risco de erro na execução de operações; risco de falha em sistemas críticos; risco de fraude interna ou externa; risco de perda de funcionários-chave; risco de falha de prestadores de serviços terceirizados.
5. **Risco de compliance:** Risco de violação de limites regulamentares; risco de não conformidade com políticas internas; risco de inadequação de investimentos ao perfil do cliente; risco de violação de informações privilegiadas; risco de não cumprimento de obrigações de PLD/FT.

11.2.MENSURAÇÃO E MONITORAMENTO

A mensuração adequada de riscos permite tomada de decisões informadas e implementação de controles proporcionais aos riscos identificados. Sem mensuração adequada, é impossível determinar se os riscos estão em níveis aceitáveis ou se ações corretivas são necessárias.

11.2.1. Métricas:

As métricas de risco são adequadas ao tipo de carteira e estratégia, fornecendo informações relevantes para gestão. São métricas aplicadas pela JPG GESTÃO DE RECURSOS LTDA:

1. **VaR (Value at Risk):** Cálculo diário de VaR para cada carteira com horizonte de 1 dia e confiança de 95%; VaR histórico baseado em 252 dias úteis de observações; VaR paramétrico para carteiras com distribuição normal de retornos; VaR Monte Carlo para carteiras com instrumentos complexos; comparação de VaR realizado versus VaR estimado (backtesting).
2. **Stress testing:** Cenário de alta de juros de 200 basis points para carteiras de renda fixa; cenário de queda de 20% no Ibovespa para carteiras de ações; cenário de desvalorização cambial de 30% para exposições em dólar; cenário de crise de liquidez com spreads ampliados; cenário de default de maior emissor da carteira.
3. **Análise de cenários:** Cenário base, otimista e pessimista para performance das carteiras; análise de impacto de mudanças na política monetária; cenário de recessão econômica e seus impactos; análise de correlações em períodos de stress; cenário de mudanças regulamentares significativas.
4. **Concentração por emissor/setor:** Monitoramento diário de concentração por emissor com limite máximo de 5%; análise semanal de concentração setorial com limite de 25% por setor; monitoramento de concentração geográfica para investimentos internacionais; análise de concentração por rating de crédito; monitoramento de concentração por prazo de vencimento.

11.2.2. Relatórios:

Relatórios estruturados de risco garantem que informações relevantes cheguem aos tomadores de decisão no momento adequado. Comunicação efetiva de riscos permite ações tempestivas e mantém todos os stakeholders informados sobre exposições. São relatórios da JPG GESTÃO DE RECURSOS LTDA:

1. **Relatório diário de risco:** Dashboard com VaR de todas as carteiras; semáforo de risco com indicadores visuais por nível de exposição; alertas para violações de limites; gráficos de evolução de risco ao longo do tempo; comparação de risco realizado versus estimado.
2. **Relatório semanal para gestores:** Análise detalhada de performance ajustada ao risco por carteira;

decomposição de fontes de risco (mercado, crédito, liquidez); análise de contribuição de cada ativo para o risco total; comparação com benchmarks e pares; recomendações para otimização de risco-retorno.

3. **Relatório mensal para Alta Administração:** Resumo executivo de exposições de risco consolidadas; análise de tendências de risco ao longo do mês; relatório de exceções e violações de limites; análise de adequação de limites versus estratégia; proposta de ajustes em políticas de risco.
4. **Relatório trimestral para acionistas:** Avaliação abrangente da efetividade do framework de risco; análise de correlações e concentrações não intencionais; revisão de metodologias de mensuração de risco; benchmarking com práticas de mercado; proposta de melhorias no sistema de gestão de risco.

11.3.LIMITES E CONTROLES

Os limites de risco são instrumentos fundamentais de governança que traduzem o apetite ao risco da JPG GESTÃO DE RECURSOS LTDA em parâmetros operacionais concretos. Limites bem definidos e monitorados evitam exposições excessivas e garantem que os riscos assumidos estejam alinhados com a estratégia e capacidade da organização.

11.3.1. Definição de Limites:

A definição de limites deve considerar múltiplos fatores, incluindo apetite ao risco, regulamentação, características dos investidores e condições de mercado.

1. **Aprovação pela Alta Administração:** Limite de VaR consolidado de 2% do patrimônio líquido aprovado trimestralmente; limite de concentração por emissor de 5% aprovado anualmente; limite de exposição cambial de 10% aprovado conforme estratégia; limite de alavancagem máxima de 1,5x aprovado pelo Diretor Presidente, Diretor de Compliance e Diretor de Riscos; revisão de limites após eventos de mercado significativos.
2. **Revisão periódica:** Revisão trimestral de adequação de limites versus performance; análise semestral de utilização histórica de limites; avaliação anual de limites versus apetite ao risco; revisão extraordinária após mudanças regulamentares; benchmarking anual de limites com pares do mercado.
3. **Comunicação clara aos gestores**: Manual de limites atualizado e distribuído a todos os gestores; treinamento específico sobre limites para novos funcionários; sistema automatizado que mostra limites disponíveis em tempo real; alertas por e-mail quando limites atingem 80% da utilização; reunião mensal para discussão de limites e exceções.
4. **Documentação de exceções:** Formulário padronizado para solicitação de exceções temporárias; aprovação obrigatória da Alta Administração para exceções; prazo máximo de 5 dias úteis para regularização; relatório mensal de exceções para a Alta Administração; análise de causas raiz para exceções recorrentes.

12. CONTROLES DE COMPLIANCE

Os controles de compliance garantem que a JPG GESTÃO DE RECURSOS LTDA opere dentro do arcabouço regulamentar aplicável, protegendo tanto a empresa quanto os investidores de riscos regulamentares e reputacionais.

12.1.MONITORAMENTO REGULAMENTAR

O ambiente regulamentar do mercado de capitais é dinâmico, com mudanças frequentes que podem impactar significativamente as operações da JPG GESTÃO DE RECURSOS LTDA. Monitoramento proativo de mudanças regulamentares permite adaptação tempestiva e evita violações não intencionais.

12.1.1. Acompanhamento de Mudanças:

O acompanhamento sistemático de mudanças regulamentares deve cobrir todas as esferas que podem impactar a atividade de gestão de carteiras. São acompanhamentos adotados pela JPG GESTÃO DE RECURSOS LTDA:

1. **Normas CVM:** Assinatura de newsletter oficial da CVM; monitoramento diário do site da CVM para novas publicações; participação em consultas públicas relevantes; análise de impacto de novas resoluções e instruções; cronograma de implementação de mudanças regulamentares.
2. **Regulamentação do Banco Central:** Acompanhamento de mudanças em regulamentação cambial que afeta investimentos internacionais; monitoramento de alterações em regras de derivativos; análise de impacto de mudanças na política monetária; acompanhamento de regulamentação sobre PLD/FT; monitoramento de mudanças em regras de capital.
3. **Legislação tributária**: Acompanhamento de mudanças em tributação de investimentos; análise de impacto de novas regras de IR para fundos; monitoramento de alterações em IOF; acompanhamento de mudanças em tributação de não residentes; análise de acordos tributários internacionais.
4. **Outras regulamentações aplicáveis:** Monitoramento de mudanças na LGPD que afetam tratamento de dados; acompanhamento de regulamentação trabalhista; monitoramento de mudanças em normas contábeis; análise de impacto de regulamentação ambiental (ESG); acompanhamento de normas de auditoria.

12.1.2. Implementação:

A implementação adequada de mudanças regulamentares requer planejamento, recursos e acompanhamento sistemático. Implementação inadequada pode resultar em violações regulamentares mesmo quando a mudança foi identificada tempestivamente.São medidas de implementação adotadas pela JPG GESTÃO DE RECURSOS LTDA:

1. **Análise de impacto:** Matriz de impacto avaliando efeitos operacionais, sistêmicos e de custos; análise de gap entre práticas atuais e novos requisitos; identificação de recursos necessários para implementação; cronograma detalhado de implementação; análise de riscos de não conformidade.
2. **Plano de implementação:** Cronograma detalhado com marcos e responsáveis; orçamento específico para implementação; plano de comunicação interna sobre mudanças; treinamento específico para áreas impactadas; testes de novos procedimentos antes da implementação.
3. **Treinamento das equipes:** Sessões de treinamento específicas sobre novas regulamentações; material didático adaptado para cada função; avaliação de conhecimento após treinamento; reciclagem periódica sobre mudanças implementadas; biblioteca de consulta sobre regulamentação atualizada.
4. **Testes de conformidade:** Teste piloto de novos procedimentos em ambiente controlado; verificação de adequação de sistemas às novas exigências; teste de relatórios regulamentares com novos formatos; simulação de inspeções com base em novas regras; validação de controles implementados.

12.2.CANAL DE DENÚNCIAS

O canal de denúncias é um mecanismo fundamental para identificação de violações éticas e regulamentares, permitindo ação corretiva tempestiva. Facilita a identificação de problemas que poderiam não ser detectados pelos controles normais, protegendo tanto a organização quanto os stakeholders.

12.2.1. Estrutura:

A estrutura do canal de denúncias garante acessibilidade, confidencialidade e efetividade no tratamento das comunicações recebidas.

Canal confidencial para denúncias: caixa física lacrada em local acessível; e-mail específico monitorado por compliance;
Proteção ao denunciante: investigação imparcial de denúncias; proteção de identidade quando solicitada; acompanhamento de denunciantes para verificar ausência de retaliação; medidas corretivas para retaliação

comprovada.
Tratamento adequado das denúncias: prazo máximo de 48 horas para início da investigação; relatório formal de investigação; comunicação de resultado ao denunciante quando possível.

12.2.2. Processo:

O processo de tratamento de denúncias é estruturado, tempestivo e efetivo para garantir credibilidade do sistema. Processo bem definido garante tratamento adequado e uniforme de todas as denúncias, mantendo a confiança no sistema.

1. **Recebimento e registro:** classificação inicial por tipo e gravidade; atribuição de número de protocolo; comunicação de recebimento ao denunciante; prazo de 24 horas para registro formal.
2. **Investigação independente:** Designação de investigador sem conflito de interesse; acesso a documentos e sistemas necessários; entrevistas com pessoas relevantes; análise de evidências documentais; relatório preliminar em 15 dias úteis.
3. **Relatório de conclusão:** Relatório formal com achados e conclusões; recomendações de ações corretivas; identificação de responsabilidades; proposta de medidas preventivas;
4. **Acompanhamento de ações corretivas:** Cronograma de implementação de ações corretivas; responsável designado para cada ação; acompanhamento mensal do progresso; verificação de efetividade das ações; relatório final de encerramento.

13. CONTROLES DE INVESTIMENTO

Os controles de investimento são específicos para a atividade principal da JPG GESTÃO DE RECURSOS LTDA, garantindo que as decisões de investimento sejam tomadas de forma adequada, documentada e alinhada com os objetivos dos investidores.

13.1.PROCESSO DE DECISÃO

O processo de decisão de investimento deve refletir o dever fiduciário da JPG GESTÃO DE RECURSOS LTDA para com seus clientes, priorizando sempre os interesses dos investidores. Processo estruturado garante consistência, rastreabilidade e adequação das decisões de investimento.

13.1.1. Análise de Investimentos:

A análise de investimentos deve ser rigorosa, documentada e baseada em metodologias consistentes que permitam comparação e avaliação posterior. São procedimentos da JPG GESTÃO DE RECURSOS LTDA:

1. **Metodologia padronizada:** Template padrão de análise com seções obrigatórias (tese de investimento, análise financeira, riscos, preço-alvo); checklist de itens mínimos a serem analisados; metodologia de valuation consistente por setor; critérios padronizados de rating interno; processo de peer review para análises complexas.
2. **Due diligence adequada:** Análise detalhada de demonstrações financeiras dos últimos 3 anos; verificação de informações junto a fontes independentes; análise de governança corporativa do emissor; avaliação de riscos ESG; consulta a agências de rating e research houses.
3. **Documentação completa:** Relatório formal de análise arquivado no sistema; planilhas de valuation com premissas claramente identificadas; atas de reuniões de análise; e-mails de discussão sobre investimentos; arquivo de materiais de suporte (apresentações, relatórios externos).
4. **Aprovação conforme alçadas:** Investimentos até R$ 1 milhões aprovados por gestor sênior; investimentos até R$ 5 milhões aprovados por diretor; investimentos acima de R$ 5 milhões aprovados pela Alta Administração; Operações em mercados internacionais, novos emissores ou ativos não previstos na política deverão ser aprovados pela Alta Administração; aprovação documentada com justificativa.

13.1.2. Execução:

A execução de investimentos deve ser controlada para garantir que seja feita conforme as decisões aprovadas e dentro dos melhores padrões de mercado. São procedimentos da JPG GESTÃO DE RECURSOS LTDA:

1. **Ordens claras e documentadas:** Ordem por escrito especificando ativo, quantidade, preço limite e prazo; confirmação de recebimento da ordem pelo operador; gravação de ordens telefônicas; sistema eletrônico de ordens com trilha de auditoria; arquivo de todas as ordens por prazo regulamentar.
2. **Execução por pessoa autorizada:** Lista atualizada de operadores autorizados; certificação obrigatória para operadores; sistema de senhas individuais para execução; dupla confirmação para operações acima de determinado valor; log de todas as execuções com identificação do operador.
3. **Verificação de melhor execução:** Comparação de preços executados com cotações de mercado; análise de spread bid-ask no momento da execução; verificação de volume executado versus disponível; análise de impacto de mercado das operações; relatório mensal de qualidade de execução.
4. **Confirmação independente:** Back office confirma detalhes de todas as operações; reconciliação entre ordens dadas e operações executadas; confirmação de settlement com custodiante; verificação de preços com fontes independentes; relatório diário de operações para gestores.

13.2.MONITORAMENTO DE PERFORMANCE

O monitoramento de performance é essencial para avaliar a qualidade das decisões de investimento e prestar contas adequadamente aos investidores. Permite identificação tempestiva de problemas, ajustes de estratégia e transparência com investidores.

13.2.1. Métricas:

As métricas de performance devem ser abrangentes, comparáveis e relevantes para os objetivos de cada carteira. São métricas adotadas pela JPG GESTÃO DE RECURSOS LTDA:

1. **Retorno absoluto e relativo:** Cálculo diário de retorno de cada carteira; comparação com benchmark específico para cada estratégia; análise de tracking error versus benchmark; cálculo de alpha e beta das carteiras; análise de performance em diferentes períodos (1 mês, 3 meses, 1 ano, desde o início).
2. **Indicadores de risco-retorno:** Índice de Sharpe para cada carteira e período; volatilidade anualizada das carteiras; drawdown máximo e atual; VaR realizado versus estimado; correlação com mercado e outros ativos.
3. **Attribution analysis:** Decomposição de performance entre asset allocation e security selection; contribuição de cada ativo para performance total; análise de timing de entrada e saída de posições; impacto de custos de transação na performance; análise de performance por setor ou região.
4. **Benchmark adequado:** CDI para carteiras de renda fixa conservadoras; Ibovespa para carteiras de ações; índices compostos para carteiras mistas; benchmarks customizados para estratégias específicas; revisão anual de adequação de benchmarks.

13.2.2. Relatórios:

Os relatórios de performance devem ser claros, tempestivos e adequados às necessidades de cada tipo de investidor. Comunicação efetiva de performance mantém investidores informados e demonstra transparência na gestão. São relatórios adotados pela JPG GESTÃO DE RECURSOS LTDA:

1. **Relatório diário para gestores:** Dashboard com performance de todas as carteiras; alertas para performance significativamente diferente do esperado; análise de contribuição dos principais ativos; comparação com benchmarks; identificação de carteiras que requerem atenção.

2. **Relatório mensal para investidores:** Relatório padronizado com performance, composição da carteira e comentários do gestor; gráficos de evolução de performance e comparação com benchmark; análise de riscos e exposições; perspectivas para o próximo período; glossário de termos técnicos.
3. **Relatório trimestral detalhado:** Análise abrangente de performance e fatores que a influenciaram; revisão de estratégia e posicionamento; análise de cenários e perspectivas; comparação com pares e mercado; discussão de mudanças em políticas ou estratégias.
4. **Apresentação anual para investidores:** Apresentação presencial ou virtual com performance anual; análise de cumprimento de objetivos estabelecidos; discussão de lições aprendidas e melhorias implementadas; perspectivas para o próximo ano; sessão de perguntas e respostas.

14. GESTÃO DE INCIDENTES

A gestão de incidentes é fundamental para resposta rápida e efetiva a eventos que possam impactar as operações, clientes ou conformidade regulamentar da JPG GESTÃO DE RECURSOS LTDA.

14.1.IDENTIFICAÇÃO E CLASSIFICAÇÃO

A identificação tempestiva e classificação adequada de incidentes são críticas para acionamento de resposta apropriada e minimização de impactos. Resposta rápida pode ser a diferença entre um incidente menor e uma crise significativa.

14.1.1. Tipos de Incidentes:

A JPG GESTÃO DE RECURSOS LTDA está preparada para responder a diversos tipos de incidentes que podem afetar suas operações. São eles:

1. **Operacionais:** Falha em sistemas críticos de gestão de carteiras; erro significativo em execução de operações; perda de dados ou corrupção de arquivos; indisponibilidade de prestadores de serviços críticos; problemas de conectividade com mercados ou custodiantes.
2. **Regulamentares:** Violação não intencional de limites regulamentares; falha em reportar informações obrigatórias; identificação de não conformidade com políticas internas; comunicação inadequada com órgãos reguladores;
3. **Segurança da informação:** Tentativa de invasão de sistemas; vazamento de informações confidenciais; perda ou roubo de equipamentos com dados sensíveis; acesso não autorizado a informações privilegiadas; ataques de malware ou ransomware.
4. **Fraude ou conduta inadequada:** Suspeita de uso de informações privilegiadas; identificação de conflitos de interesse não declarados; suspeita de manipulação de preços; violação de políticas éticas; comportamento inadequado de funcionários.

14.1.2. Classificação:

A classificação adequada de incidentes permite acionamento de resposta proporcional e alocação adequada de recursos. Classificação incorreta pode resultar em resposta inadequada, seja por excesso ou por deficiência. As classificações da JPG GESTÃO DE RECURSOS LTDA são:

1. **Criticidade (baixa, média, alta):** Baixa - erro em relatório interno sem impacto externo; Média - violação menor de limite com correção imediata; Alta - falha de sistema crítico afetando múltiplas carteiras; Crítica - suspeita de fraude ou vazamento de informações privilegiadas.
2. **Impacto (local, regional, sistêmico):** Local - problema afetando uma carteira específica; Regional - problema afetando múltiplas carteiras ou clientes; Sistêmico - problema afetando toda a operação ou com potencial impacto regulamentar; Reputacional - problema com potencial impacto na imagem da empresa.

3. **Urgência (imediata, alta, normal):** Imediata - sistema crítico fora do ar durante horário de mercado; Alta - violação regulamentar que requer comunicação no mesmo dia; Normal - problema que pode ser resolvido dentro de prazos normais; Planejada - problema que permite planejamento de resposta.

14.2.PROCESSO DE RESPOSTA

O processo de resposta deve ser estruturado, rápido e efetivo para minimizar impactos e restaurar operações normais. Processo bem definido garante resposta consistente e adequada independentemente do tipo de incidente.

14.2.1. Acionamento:

O acionamento adequado garante que as pessoas certas sejam notificadas no momento certo para resposta efetiva. São acionamentos praticados na JPG GESTÃO DE RECURSOS LTDA:

1. **Comunicação imediata:** Sistema automatizado de alertas para incidentes críticos; lista de contatos atualizada para diferentes tipos de incidentes; múltiplos canais de comunicação (telefone, e-mail, SMS); procedimento para acionamento fora do horário comercial; escalação automática se não houver resposta.
2. **Equipe de resposta:** representantes das áreas críticas; líder de incidente designado conforme tipo e gravidade; especialistas técnicos disponíveis para consulta; autoridade para tomar decisões rápidas; comunicador designado para stakeholders externos.
3. **Documentação inicial:** Registro imediato do incidente com horário e circunstâncias; identificação preliminar de impactos; lista inicial de ações tomadas; identificação de recursos necessários; estimativa preliminar de tempo para resolução.

14.2.2. Investigação:

A investigação adequada é essencial para compreender causas, implementar correções e prevenir recorrências. Investigação superficial pode deixar causas raiz não resolvidas, resultando em incidentes recorrentes. São classificações de investigação da JPG GESTÃO DE RECURSOS LTDA:

1. **Análise de causa raiz:** Metodologia estruturada (5 porquês, diagrama de Ishikawa); análise de fatores contribuintes; identificação de falhas em controles; avaliação de fatores humanos e sistêmicos; documentação detalhada de achados.
2. **Coleta de evidências:** Preservação de logs de sistemas; coleta de documentos relevantes; entrevistas com pessoas envolvidas; análise forense quando necessário; cadeia de custódia para evidências críticas.
3. **Relatório de investigação:** Relatório formal com cronologia detalhada; identificação de causas raiz e fatores contribuintes; avaliação de adequação de controles existentes; recomendações específicas e acionáveis; aprovação por autoridade competente.

15. DOCUMENTAÇÃO E REGISTRO

A documentação adequada é fundamental para demonstrar conformidade, facilitar auditorias e garantir continuidade operacional.

15.1.POLÍTICAS E PROCEDIMENTOS

A Resolução CVM 21/2021 exige documentação adequada de políticas e procedimentos de controles internos. Documentação inadequada pode resultar em penalizações regulamentares e dificultar operações eficientes.

15.1.1. Estrutura:

A estrutura da documentação deve ser lógica, consistente e facilitar consulta e atualização. Na JPG GESTÃO DE RECURSOS LTDA adotamos:

1. **Hierarquia clara:** Políticas de alto nível aprovadas pela Alta Administração; procedimentos operacionais detalhados por área; instruções de trabalho específicas por função; formulários e templates padronizados; glossário de termos técnicos.
2. **Versionamento:** Controle rigoroso de versões com numeração sequencial; registro de alterações com data e responsável; aprovação formal de novas versões; comunicação de mudanças para áreas afetadas; arquivo de versões anteriores por prazo regulamentar.
3. **Aprovação formal:** Assinatura de aprovação por autoridade competente; ata de reunião registrando aprovação; processo formal de revisão antes da aprovação; validação técnica por áreas especialistas; comunicação oficial de entrada em vigor.
4. **Distribuição controlada:** Lista de distribuição atualizada para cada documento; controle de acesso conforme necessidade de conhecer; sistema eletrônico de distribuição com confirmação de recebimento; treinamento obrigatório sobre novos procedimentos; recolhimento de versões obsoletas.

15.1.2. Atualização:

A documentação deve ser mantida atualizada para refletir mudanças operacionais, regulamentares e de melhores práticas. Documentação desatualizada pode levar a execução incorreta de controles e não conformidades. São rotinas que adotamos na JPG GESTÃO DE RECURSOS LTDA:

1. **Revisão periódica:** Cronograma anual de revisão de todas as políticas; revisão extraordinária após mudanças regulamentares; feedback de usuários sobre adequação de procedimentos; benchmarking com melhores práticas; atualização baseada em lições aprendidas.
2. **Processo de mudança:** Solicitação formal de mudança com justificativa; análise de impacto das mudanças propostas; aprovação por autoridade competente; comunicação prévia de mudanças; treinamento sobre alterações implementadas.
3. **Comunicação de alterações:** E-mail formal comunicando mudanças; destaque de alterações em nova versão; reunião de comunicação para mudanças significativas; prazo de transição quando necessário; confirmação de recebimento e entendimento.

15.2.REGISTROS OPERACIONAIS

Os registros operacionais são evidências da execução adequada de controles e são essenciais para auditorias internas e externas. Registros inadequados podem impossibilitar demonstração de conformidade mesmo quando controles são executados adequadamente.

15.2.1. Retenção:

Os prazos de retenção devem atender requisitos regulamentares e necessidades operacionais da JPG GESTÃO DE RECURSOS LTDA.

1. **Prazos regulamentares:** Registros de operações mantidos por 10 anos conforme regulamentação CVM; documentos de PLD/FT retidos por 10 anos; registros contábeis conforme legislação fiscal; correspondência com clientes por 5 anos; atas de reuniões por prazo indefinido.
2. **Organização adequada**: Sistema de arquivamento por data, cliente ou tipo de documento; indexação que facilite localização; backup de documentos eletrônicos; arquivo físico organizado e seguro; inventário periódico de documentos arquivados.
3. **Acesso controlado:** Controle de acesso baseado em necessidade de conhecer; log de consultas a documentos sensíveis; aprovação para acesso a arquivos confidenciais; restrição física a áreas de arquivo; controle de retirada e devolução de documentos.

4. **Backup e recuperação:** Backup diário de documentos eletrônicos; armazenamento de backup em local seguro e separado; teste periódico de recuperação de documentos; redundância para documentos críticos; plano de recuperação em caso de desastre.

16. DISPOSIÇÕES FINAIS

16.1. VIGÊNCIA E ATUALIZAÇÃO

16.1.1. Vigência

Esta política entra em vigor na data de sua aprovação pela Alta Administração.

16.1.2. Revisão Periódica

Esta política deve ser revisada:

- Anualmente, no mínimo;
- Sempre que houver mudança relevante em regulamentação;
- Sempre que houver mudança significativa nos processos operacionais;
- Sempre que identificada deficiência que requeira atualização.

16.1.3. Aprovação de Alterações

Alterações a esta política devem ser aprovadas pela Alta Administração e comunicadas a todos os colaboradores.

16.2. RESPONSABILIDADES

As responsabilidades devem ser claramente definidas para garantir implementação e manutenção adequada dos controles internos. Responsabilidades claras garantem accountability e execução adequada dos controles.

1. **Alta administração:** Aprovação e revisão periódica da política; alocação de recursos adequados; definição do tom no topo; supervisão da efetividade dos controles; responsabilidade final por conformidade regulamentar.
2. **Gestores de área:** Implementação de controles em suas áreas; treinamento de equipes; monitoramento de efetividade; comunicação de problemas; melhoria contínua de processos.
3. **Funcionários:** Execução adequada de controles; comunicação de problemas identificados; participação em treinamentos; aderência a políticas e procedimentos; colaboração com auditorias.
4. **Compliance:** Monitoramento de conformidade; atualização de políticas; coordenação de treinamentos; investigação de violações; comunicação com reguladores.

Documento assinado digitalmente por:

PEDRO HENRIQUE LIMA DE OLIVEIRA
080.143.809-83
2025-11-24T17:57:49.349676

_____

Pedro Henrique Lima de Oliveira
Diretor de Gestão de Recursos
JPG GESTÃO DE RESCURSOS LTDA

Documento assinado digitalmente
GUILHERME MEI CARRASCO
Data: 25/11/2025 08:07:03-0300
Verifique em https://validar.iti.gov.br

_____

Guilherme Mei Carrasco
Diretor de Riscos, Compliance e PLD-FTP.
JPG GESTÃO DE RESCURSOS LTDA