HΣMΣRA

# Política de Conformidade e Controles Internos

# Sumário

## Introdução

Esta Política de Conformidade (*Compliance*) e Controles Internos ("Política") dispõe sobre o propósito da função de conformidade e controles internos estabelecida pela HEMERA Distribuidora de Títulos e Valores Mobiliários LTDA ("HEMERA DTVM").

Estes requerimentos, enfatizam as responsabilidades da administração da HEMERA DTVM, pela manutenção de uma adequada função de conformidade, de acordo com os padrões de boas práticas de governança corporativa, compatíveis à natureza das atividades da HEMERA DTVM e de seus processos, com a complexidade de seus produtos/serviços e respectivos perfis de risco, bem como, do porte e estrutura da-HEMERA DTVM.

Os itens deste documento constituem um importante instrumento a todos colaboradores e todos que, de alguma forma, auxiliam, direta ou indiretamente, o desenvolvimento das atividades da HEMERA DTVM para apoio nas ações e, abordam as premissas para a implementação da estrutura organizacional e as atividades relacionadas à função de conformidade, que assegurem a observância e a devida aplicação da legislação vigente, da regulamentação e recomendações de órgãos supervisores externos e, quando aplicáveis, dos códigos de ética e conduta e de outras normas internas da HEMERA DTVM.

## Objetivo

Tem como objetivo regulamentar a Política de Conformidade (*Compliance*) e Controles Internos aplicável à HEMERA DTVM.

A função de conformidade é estruturada para o exercício das atividades, de forma independente e com autoridade, por profissionais treinados e com experiência e utilização de metodologia adequada, a fim de que sejam capazes de avaliar os descumprimentos de dispositivos legais e regulamentares na condução dos processos operacionais e de negócios realizados pelas áreas da HEMERA DTVM.

Assegurar que a gestão dos negócios seja executada em conformidade com as diretrizes estabelecidas e com os regulamentos emanados por órgãos oficiais, bem como fazer com que as regras internas e os controles vigentes na organização sejam conhecidos e cumpridos.

O propósito de "*Compliance*" é a de garantir o perfeito funcionamento do Sistema de Controles Internos da HEMERA DTVM, procurando reduzir os riscos de acordo com a complexidade dos seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento das leis, normas internas e externas existentes.

Desta forma é necessário que a HEMERA DTVM reestruture suas estratégias organizacionais e tecnológicas, visando fortalecer a política de controles internos, o código de ética e normas de conduta, alinhando seus processos para assegurar o cumprimento das normas e procedimentos determinados pelos órgãos reguladores, e principalmente, preservar imagem perante o mercado.

Visando o cumprimento integral do programa de conformidade da HEMERA DTVM, recomendamos que o presente documento seja lido conjuntamente com o Código de Ética e Conduta da instituição, além do conjunto de políticas relacionadas ao gerenciamento de riscos.

## Conformidade com a LGPD

A HEMERA DTVM reconhece a importância da proteção dos dados pessoais e está comprometida com a observância integral da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Neste contexto, a instituição adota medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações de destruição, perda, alteração, comunicação ou difusão indevida, conforme previsto no artigo 46 da LGPD.

As práticas da HEMERA DTVM quanto ao tratamento de dados pessoais seguem os princípios previstos no artigo 6º da LGPD, destacando-se:

- ✓ A finalidade e necessidade do tratamento;
- ✓ A adequação e transparência das operações;
- ✓ A segurança, prevenção e responsabilização.

Todos os dados pessoais tratados pela HEMERA DTVM são coletados com base em fundamentos legais (arts. 7º e 11 da LGPD), observando o legítimo interesse da instituição ou o consentimento do titular, quando aplicável.

Além disso, a HEMERA DTVM:

Garante os direitos dos titulares de dados, conforme artigo 18 da LGPD, disponibilizando canal apropriado para requisições, correções, revogação de consentimento e acesso às informações;

Realiza, quando aplicável, o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) nos termos do artigo 38;

Mantém estrutura de governança de privacidade com suporte da área de compliance e controles internos, alinhada às boas práticas de proteção de dados.

O tratamento de dados por terceiros, parceiros ou operadores é regido por cláusulas contratuais que asseguram o cumprimento da LGPD, incluindo responsabilidades e medidas de segurança adequadas (art. 39 da LGPD).

Todos os colaboradores devem seguir as diretrizes desta Política e dos normativos internos relacionados à privacidade e proteção de dados, sendo sua observância obrigatória e sujeita a medidas disciplinares em caso de descumprimento.

## Glossário

**LGPD** - Lei nº 13.709/2018 que regula o tratamento de dados pessoais por pessoas físicas ou jurídicas.

**Resolução BCB nº 85/2021** - Norma que estabelece requisitos de segurança cibernética e gestão de riscos operacionais em instituições financeiras

**Compliance** - Conjunto de práticas voltadas à conformidade com leis, regulamentos e normas internas.

**DPO (Encarregado) -** Pessoa indicada para atuar como canal de comunicação entre controlador, titulares e ANPD.

**RIPD (Relatório de Impacto à Proteção de Dados)** - Documento exigido em certos casos que demonstra as medidas tomadas para mitigar riscos aos dados pessoais.

**Canal de Ética / Denúncias** - Meio formal para relatar desvios de conduta, violações à lei ou políticas internas.

**Controles Internos -** Sistemas, processos e procedimentos que asseguram o cumprimento das normas e a integridade das operações.

**Autoavaliação de Riscos** - Processo periódico para identificação e medição dos riscos internos pelas áreas responsáveis.

**Gestão da Continuidade de Negócios -** Planejamento para manter ou recuperar operações críticas diante de eventos disruptivos.

**Segregação de Funções** - Prática que evita conflito de interesses ao separar responsabilidades operacionais e decisórias.

**Segurança Cibernética -** Conjunto de práticas e tecnologias para proteger sistemas, redes e dados contra ataques ou acessos indevidos.

**Controle de Acesso Lógico** - Restrição de acesso a sistemas ou dados com base em autenticação e perfis de usuário.

**Log de Acesso -** Registro das atividades dos usuários em sistemas, essencial para auditorias e investigações.

**Plano de Resposta a Incidentes** - Procedimento formal para detecção, resposta e recuperação de incidentes cibernéticos.

**Teste de Vulnerabilidades** - Ações que simulam ataques para identificar falhas de segurança nos sistemas.

**Ton at the top** - termo em inglês significa “exemplo vem de cima” e mostra que uma gestão corporativa de sucesso deve ter como exemplo os líderes da governança.

## Público-Alvo

Esta Política contém informações indispensáveis para os Colaboradores envolvidos nos processos que envolvam as operações da HEMERA DTVM.

Está disponível em um portal corporativo com amplo acesso para qualquer Colaborador efetuar consulta.

Todos os Colaboradores em razão de suas funções na HEMERA DTVM, devem se assegurar do entendimento das legislações e normas aplicáveis e em caso de dúvida devem buscar auxílio junto a área de *compliance* e controles internos. A alegação de desconhecimento das regras não será aceita como justificativa no caso de quaisquer desconformidades com esta Política.

**Definições**

**Risco de Conformidade (*Compliance*)**

É o risco de sanções legais ou regulatórias, de perda financeira ou risco de imagem (reputação), que a instituição pode sofrer como resultado da falha no cumprimento da aplicação de leis, normas e regulamentos internos.

**Sistema de Controles internos**

É o processo de mapeamento de processos, controles e riscos compreendendo inclusive, métodos e medidas adotadas para salvaguardar os ativos, verificar a exatidão e fidelidade dos dados contábeis, desenvolver a eficiência nas operações e estimular o cumprimento das políticas e estratégias da instituição.

O sistema de controle interno é o ordenamento de regras que determina o cumprimento dos seguintes aspectos:

- ✓ Implantação do processo de acompanhamento do estrito cumprimento das normas e regulamentações vigentes;
- ✓ Definição das responsabilidades quanto a controles internos, atribuídas aos diversos níveis da organização;
- ✓ Segregação das atividades de classificação de risco das demais atividades;
- ✓ Identificação de potenciais conflitos de interesses;
- ✓ Identificação e avaliação de fatores de riscos internos e externos;
- ✓ Acessibilidade dos controles internos e *compliance* a todos os Colaboradores.

O processo de controles internos é considerado como sendo dinâmico e constante. Parte importante deste processo é a existência da documentação de controles em políticas e procedimentos, assim como um adequado processo de aprovação de novos produtos e de transações relevantes.

A determinação da qualidade do ambiente de controles internos é adotada em função da maneira como os Colaboradores aderem às políticas/procedimentos existentes, e do quão claramente são identificadas e endereçadas deficiências em relação às mesmas. Sendo assim, o modelo de controles internos visa:

- ✓ Garantir a aderência a políticas e procedimentos: Para atingir este objetivo a área de *compliance* e controles internos efetua a revisão de políticas institucionais, participa ativamente do processo de adequação aos requerimentos regulatórios, garante que toda e qualquer nova normativa que surja seja devidamente analisada e implementada, sempre que cabível a instituição, atua na melhoria de processos por meio de mapeamentos dos processos e fluxos operacionais juntos a 1ª linha de defesa, principalmente junto a figura dos gestores, participa das reuniões de gestão de riscos, além de acompanhar as auditorias e as deficiências identificadas.
- ✓ Atuar na identificação de novos riscos: Para tanto, a área de *compliance*, controles internos e a Gestão de Riscos revisa, no mínimo anualmente, os processos das áreas de negócios, sempre questionando e apontando se estes estão dentro do apetite a riscos da instituição, se fazem parte dos objetivos estratégicos ou se são inerentes aos objetivos do processo.
- ✓ Por fim, a área de *compliance* e controles internos, junto a alta administração, é responsável pela melhoria da qualidade do ambiente de controle, proporcionando visão horizontal da organização sobre os principais temas relacionados a esta. Caso as ações de controles internos revelem deficiências críticas, recorrentes ou com possibilidade de geração de benefícios para a instituição, elas são priorizadas e tornam-se ações de melhorias de processos, as quais complementam os pilares da estrutura da área de *compliance* e controles internos.

No processo de monitoramento das atividades é importante o entendimento da diferença conceitual entre:

**Deficiência** - Falha no atendimento de um requisito, ou imperfeição, ou carência, inclusive quanto à segurança do sistema, dos serviços e dos resultados esperados.

**Não Conformidade** - É o não atendimento de um requisito especificado na legislação e/ou nos normativo internos e abrange o afastamento ou ausência de uma ou mais características de controle.

**Estrutura Funcional de *Compliance* e Controles Internos**

A HEMERA DTVM possui uma estrutura compatível para promover o efetivo cumprimento das regras de controles internos e *compliance* que se reporta diretamente à Diretoria Executiva, para fins institucionais, haja vista a completa autonomia da diretoria responsável por *compliance* e controles internos e do Comitê de *Compliance* e Risco, cujas regras de composição, responsabilidades, periodicidade das reuniões se encontram no Código de Ética e Conduta.

**Atribuições e responsabilidades**

**Diretoria Executiva**

- ✓ Deliberar sobre a divisão das responsabilidades das pessoas envolvidas na função de conformidade;
- ✓ Aprovar formalmente esta Política, os processos, os procedimentos e os sistemas necessários à implementação da função de conformidade (controles internos e *compliance*), respeitada a autonomia da diretoria responsável por *compliance* e controles internos e do Comitê de *Compliance* e Risco;
- ✓ Assegurar que a presente Política seja compatível com a complexidade, a estrutura, o perfil de risco da HEMERA DTVM;
- ✓ Garantir a comunicação da política de conformidade a todos os Colaboradores;
- ✓ Prover a alocação de pessoal em quantidade suficiente, adequadamente treinado e com experiência necessária para o exercício das atividades relacionadas com a função de conformidade;
- ✓ Assegurar as medidas necessárias para garantir independência e adequada autoridade aos responsáveis por atividades relacionadas com a função de conformidade na HEMERA DTVM;
- ✓ Assegurar a alocação de recursos suficientes para o desempenho das atividades relacionadas com a função de conformidade;

- ✓ Assegurar o livre acesso dos responsáveis por atividades relacionadas com a função de conformidade às informações necessárias para o exercício de suas atribuições;
- ✓ Assegurar a independência funcional da área de Compliance e Controles Internos, garantindo livre acesso às informações, sistemas e pessoas necessárias à execução de suas atribuições;
- ✓ Cientificar-se dos resultados decorrentes das atividades relacionadas com a função de conformidade, de possíveis irregularidades ou falhas identificadas e garantir que medidas corretivas sejam tomadas;
- ✓ Estabelecer uma cultura organizacional com ênfase na relevância dos sistemas de controles internos e no engajamento de cada funcionário no processo de controle interno, reforçando o "*Tone from the top*" como elemento essencial da integridade corporativa;
- ✓ Disseminar padrões de integridade e conduta ética como parte da cultura da instituição.

**Compliance e Controles Internos**

- ✓ Implementar as diretrizes relativas aos sistemas de controles internos aprovadas pela Diretoria;
- ✓ Certificar-se da aderência e do cumprimento das leis e outras normas externas e internas, por meio de acompanhamento das atividades diárias e objetivando identificar deficiências e não conformidades nas atividades executadas pelos Colaboradores e gestores de cada processo;
- ✓ Implantar o conceito de controles internos através de uma metodologia de *compliance*, visando melhoria nos controles e redução do risco de conformidade;
- ✓ Estabelecer os processos para o desenvolvimento de atividades de gerenciamento de riscos de conformidade incorridos pela HEMERA DTVM;
- ✓ Fixar medidas apropriadas para o monitoramento da adequação e da efetividade do sistema de controles internos;
- ✓ Promover padrões éticos e de integridade e estabelecer uma cultura dentro da organização que enfatize e demonstre a todos os Colaboradores a importância dos controles internos;
- ✓ Avaliar a aderência da HEMERA DTVM às recomendações dos órgãos de supervisão;

- ✓ Prestar suporte à diretoria ou aos administradores a respeito da observância e da correta aplicação das normas internas e externas, mantendo-os informados sobre as atualizações relevantes;
- ✓ Auxiliar na informação e na capacitação dos Colaboradores, em assuntos relativos à conformidade;
- ✓ Acompanhar a solução dos planos de ação para a regularização dos pontos de descumprimento de dispositivos legais e regulamentares levantados por auditores independentes;
- ✓ Assegurar que as deficiências de controles internos identificadas pelas áreas operacionais ou qualquer outra área de controle sejam comunicadas de maneira tempestiva para o adequado nível de gerência e corrigidas prontamente;
- ✓ Elaborar relatório anual com os resultados das atividades relacionadas com a função de conformidade (conclusões, recomendações e providências tomadas pela administração da HEMERA DTVM);
- ✓ Elaborar o relatório anual para acompanhamento sistemático das atividades relacionadas com os sistemas de controles internos;
- ✓ Controlar e divulgar internamente toda regulamentação que exija das áreas envolvidas a adoção de novos procedimentos e controles internos;
- ✓ Assegurar a existência de procedimentos adequados que identifiquem problemas de controles e potenciais riscos;
- ✓ Manter permanente acompanhamento no controle das atividades de segregação de função, processos e hierarquia de aprovação e formalização das operações, verificações e reconciliações, através de avaliações periódicas nas áreas da organização;
- ✓ Assegurar a manutenção / revisão dos processos operacionais;
- ✓ Implantar, disseminar e monitorar a cultura de controles internos na empresa, de acordo com os preceitos de legalidade e governança corporativa, identificando claramente as funções e responsabilidades de cada área;
- ✓ Promover testes periódicos acerca dos controles internos de cada área da empresa, avaliando-os através de evidências e fatos e recomendando melhorias;

- ✓ Avaliar e acompanhar a criação de novos produtos para a HEMERA DTVM, focando pontos que possam comprometer sua operacionalidade;
- ✓ Coordenar as práticas de prevenção à lavagem de dinheiro e financiamento ao terrorismo;
- ✓ Disseminar princípios e padrões de ética e integridade;
- ✓ Responder pelas obrigações tais como, elaboração e envio de informes periódicos e eventuais aos órgãos reguladores, na forma e periodicidade estabelecida nas instruções das respectivas entidades;
- ✓ Acompanhar e assegurar que as práticas comerciais e de prestação de serviços estejam em conformidade com os requisitos legais e regulatórios aplicáveis;
- ✓ Reportar tempestivamente à Diretoria Executiva, ao Comitê de Compliance e Risco e, quando aplicável, aos órgãos reguladores, quaisquer situações de descumprimento relevante, indícios de fraude, lavagem de dinheiro ou outras irregularidades detectadas;
- ✓ Monitorar o cumprimento das recomendações e planos de ação decorrentes de auditorias, inspeções, ou revisões de compliance, até sua efetiva implementação;
- ✓ Coordenar a elaboração, revisão periódica e atualização das políticas internas relacionadas à conformidade, controles internos, riscos, integridade e prevenção à lavagem de dinheiro;
- ✓ Avaliar, antes da contratação e periodicamente, a aderência de prestadores de serviço, parceiros e terceiros relevantes às políticas de compliance e aos requisitos regulatórios aplicáveis.

**Gestores e líderes de áreas**

Caberá aos gestores durante o exame:

- ✓ Mapear seus processos internos a fim de identificar e avaliar os riscos de conformidade em todas as atividades;
- ✓ Realizar autoavaliação com objetivo de identificar e mapear os riscos e os controles praticados;
- ✓ Criar e revisar periodicamente controles, visando reduzir a possibilidade de erros humanos e irregularidades em processos e sistemas, auxiliando a HEMERA DTVM a resguardar seus ativos, minimizando o risco de perdas e contravenções contra leis e regulamentações;

- ✓ Contribuir para as atividades de identificação e avaliação dos riscos inerentes aos processos de negócio sob sua responsabilidade;
- ✓ Dar a adequada resposta aos riscos de conformidade de suas áreas, processos, produtos e sistemas;
- ✓ Assegurar que todas as atividades relacionadas à função de conformidade sejam executadas e que seus resultados sejam reportados;
- ✓ Evidenciar suas afirmações com base em dados, relatórios, documentos de controle e padrões estabelecidos;
- ✓ Enfatizar o processo (modo de trabalhar, sistemas, padrões) pelos quais os resultados são obtidos.

O diretor responsável pela área de *compliance* e controles internos e o Comitê de *Compliance* e Risco exercem suas atividades de forma completamente independente das outras áreas da HEMERA DTVM.

**Procedimentos de *Compliance* e Controles Internos**

Os procedimentos de controles internos e *compliance* compreenderão atividades destinadas ao acompanhamento de atividades e/ou operações, por meio da comparação entre o que é normatizado e o realizado pelos Colaboradores da HEMERA DTVM, para que se assegure a conformidade com as regras estabelecidas.

Os Colaboradores devem acompanhar o desenvolvimento dos processos a seu cargo e comunicar eventuais ocorrências que envolvam deficiências ou não conformidades à área de *compliance* e controles internos, independente da solução imediata para o problema.

Devem ser consideradas ocorrências, para fins de reporte, as falhas no atendimento de um requisito, deficiência ou carência, inclusive quanto à segurança do sistema, dos serviços e dos resultados esperados.

Para a realização das atividades de controles internos e *compliance*, a HEMERA DTVM estabeleceu a seguinte metodologia e respectiva documentação:

- ✓ Mapeamento e documentação dos processos por meio de entrevistas com os responsáveis pela execução dos processos;
- ✓ Identificação dos riscos e pontos de controle para atividades relativas aos processos mapeados;

- ✓ Aplicação em conjunto com os responsáveis por cada área de questionários de autoavaliação dos processos e respectivas atividades para avaliação da aderência às normas internas e externas;
- ✓ Tratamento das ocorrências, ou seja, ações corretivas para as não conformidades detectadas nos processos (referenciar as normas que foram descumpridas ou não observadas).

A seguir descrevemos cada uma das responsabilidades de controles internos e *compliance*:

**Verificação do Desenho de Controles**

A área de Compliance e Controles Internos realizará, no mínimo anualmente, processo formal de verificação do desenho dos controles relacionados à segurança cibernética, segurança da informação, continuidade de negócios e contratação de serviços relevantes. Essa verificação tem como objetivo confirmar a existência, adequação e documentação formal dos controles exigidos pela regulamentação vigente, sem prejuízo das avaliações de efetividade. A verificação será baseada em evidências documentais para cada requisito normativo, registradas em checklist estruturado que contemplará, no mínimo:

- ✓ Referência normativa;
- ✓ Descrição do controle;
- ✓ Evidência apresentada;
- ✓ Conclusão da análise (Atende, Parcial, Não Atende).

  Os resultados serão reportados em relatório próprio à Diretoria Executiva, com priorização de ações corretivas para lacunas classificadas como de alta criticidade.

**Segregação de Funções e de Atividades**

Determinar a adequada segregação de funções e separação de responsabilidades, orientando o controle das atividades para evitar conflitos de interesses e para evidenciar os pontos de controle, conforme regras estabelecidas nas políticas, manuais e documentos internos da HEMERA DTVM.

Orientar à Diretoria Executiva no tocante ao organograma interno, a fim de evitar a adoção de posições conflitantes pelos Colaboradores no desempenho de suas atribuições.

Conflito de interesse é definido como uma ação ou participação (direta ou indireta) de qualquer profissional ligado à HEMERA DTVM em situação que:

- ✓ Cause influência ou prejudique a condução das tarefas profissionais;
- ✓ Possa causar prejuízo à reputação profissional ou à imagem da HEMERA DTVM;
- ✓ Propicie benefícios próprios ou a terceiros de forma exclusiva;
- ✓ Gere concorrência com a HEMERA DTVM em quaisquer atividades de negócios;
- ✓ Desvie oportunidade de negócios da HEMERA DTVM.

Todos os Colaboradores da HEMERA DTVM, no exercício de suas funções devem estar atentos a ocorrência de situação de conflito de interesses, e seguir as regras presentes no Código de Ética e Conduta.

Em hipótese alguma os Colaboradores devem recomendar profissionais qualificados a clientes ou empresas que solicitem este auxílio, visando à obtenção de benefícios pessoais ou profissionais.

Qualquer situação que caracterize ou que possa vir a acarretar situações de conflito de interesse deve ser avaliada com cuidado. Eventual ocorrência de situações descritas acima, a área de *compliance* e controles internos deve ser acionada.

Todo o Colaborador deve comunicar ao seu gestor imediato, e este levar ao conhecimento da diretoria e da área de *compliance* e controles internos, a intenção de realização de alguma das situações a seguir, sem prejuízo das informações presentes no Código de Ética e Conduta:

- ✓ Participar de um empreendimento de risco;
- ✓ Constituir um negócio próprio;
- ✓ Procurar emprego adicional;
- ✓ Prestar serviços para outra(s) Empresa(s).

Eventuais atividades paralelas, incluindo também as filantrópicas e civis, não devem ser conduzidas durante a jornada de trabalho para que não haja interferência no desempenho profissional. Além dos

itens descritos acima, todas as atividades desempenhadas internamente pelas áreas de backoffice, possuem segregação física e lógica. Os potenciais conflitos de interesse entre as atividades de Distribuição e Administração estão mitigados, visto que a HEMERA DTVM terceiriza as distribuições, só realizando as mesmas quando estritamente necessário e em favor dos interesses de seus cotistas. Para realização de distribuições, a instituição possui pessoas dedicadas em unidade separada, sem comunicação direta com as áreas de backoffice, principalmente a mesa de liquidações. Demais riscos de conflito, como recebimento e execução de ordens em nome dos fundos são mitigados por meio de controles sistêmicos que garantem a integridade do envio e recebimento das informações por parte de terceiros, não sendo possível que colaboradores realizem ou alterem ordens enviadas.

Cabe ressaltar que as estruturas dos serviços qualificados – Custódia, Escrituração e Controladoria, possuem quadro funcional e estrutura lógica totalmente segregada da área de administração fiduciária e distribuição.

**Controle e Atualização de Normas**

Cabe a área de *compliance* e controles internos o recebimento, a avaliação, a indicação das áreas envolvidas pela norma e a solicitação de adequações (revisão e publicação das normas internas adequadas).

A estrutura definida a ser seguida na organização dos documentos, contempla as seguintes responsabilidades por cada um os tipos de documentos:

**Políticas:** são atribuídas pelo nível diretivo da HEMERA DTVM e estabelecem o nível estratégico das diretrizes gerais a serem observadas por todos na organização.

**Manual de Processos:** são atribuídas aos gestores das áreas envolvidas e estabelecem o nível tático e as regras (práticas e/ou metodologias adotadas) que devem ser observadas pelas áreas operacionais para o cumprimento das diretrizes estabelecidas pelas políticas, sem prejuízo da avaliação e eventual aprovação por parte da diretoria responsável pelos gestores. Descrevem as atividades, responsáveis, evidências a serem produzidas bem como, adoção de métricas que possibilitem a medida de eficiência e de nível de serviço obtido pelo processo.

A área de *compliance* e controles internos possui a lista de documentos e controle de revisão para relacionar e controlar os documentos vigentes, em revisão, revogados, e a identificação do documento, número de sua versão, identificação de seus responsáveis, data de início de vigência, data de fim da vigência e data prevista para a sua próxima revisão, resumo de revisões realizadas identificando o que mudou entre uma versão e outra.

Esta lista e controle serão verificados, com a finalidade de promover as revisões periódicas de conteúdo e de aplicação de melhorias nos processos, sendo que haverá um prazo adequado de comunicação para que os responsáveis possam realizar a revisão antes da data de vigência do documento.

Cabe a área de *compliance* e controles internos dar apoio técnico na elaboração e atualização de normas. Esta área também é responsável por avaliar os impactos e necessidades de contemplar a atualização de outras normas vinculadas à norma que originou a revisão/elaboração.

A documentação deve ser revisada pelo menos uma vez a cada ano ou, sempre que houver mudanças significativas decorrentes de alterações na estrutura organizacional, melhorias ou simplificações em processos.

**Mapeamento de Processos**

O mapeamento dos processos permite um melhor entendimento das atividades, bem como a definição de atribuições e responsabilidades, principalmente quando aspectos interfuncionais estão envolvidos, utilizando uma metodologia de padronização adotada pela HEMERA DTVM.

Os levantamentos possibilitam conhecer as atividades que compõem o processo objeto da descrição e áreas envolvidas, conhecer a legislação pertinente, diagnosticar atividades que contribuem para a ocorrência de falhas.

Os levantamentos/mapeamentos realizados serão documentados em manuais de processos organizacionais por meio de procedimentos descritivos e/ou por fluxogramas.

**Informação e Comunicação**

A Hemera DTVM mantém canais eficazes de informação e comunicação, assegurando o acesso dos colaboradores a informações claras, confiáveis e relevantes. Os fluxos internos garantem a disseminação adequada de diretrizes e procedimentos, além da correta manutenção de dados financeiros, operacionais e de conformidade.

A instituição adota controles sobre o uso de informações externas, mantém sistemas de informação seguros e auditáveis, e realiza testes periódicos de segurança. Também possui planos de contingência e continuidade de negócios, assegurando a entrega tempestiva de informações e a qualidade dos dados processados.

**Autoavaliação de Controles e Riscos**

A Hemera DTVM adota o questionário de autoavaliação como ferramenta para mensurar a percepção dos gestores sobre o ambiente de controles e riscos operacionais. O processo permite avaliar a eficácia dos controles internos, a aderência às normas internas e externas, e o alinhamento aos objetivos estratégicos.

A autoavaliação, realizada periodicamente pelos gestores, é conduzida pela área de Compliance e Controles Internos, por meio de questionário estruturado, abrangendo:

- ✓ Cumprimento dos objetivos estratégicos;
- ✓ Conformidade legal e regulatória;
- ✓ Treinamento e conscientização em riscos operacionais;
- ✓ Gestão da continuidade de negócios.

Os resultados são analisados em conjunto com as áreas responsáveis, possibilitando a identificação de melhorias e a definição de planos de ação, com prazos e responsáveis. Os dados são registrados, monitorados e integrados à matriz de riscos e controles, sendo reportados em relatórios formais para acompanhamento contínuo.

**Monitoramento de Processos**

O monitoramento compreenderá a realização de atividades destinadas ao acompanhamento de operações e/ou dos processos, com a verificação do realizado com o planejado, para que se assegure a conformidade com as regras estabelecidas.

Serão consideradas não conformidades para fins de estabelecimento de medidas corretivas, o não atendimento de normas/regras/instruções de trabalho, a menos que as hipóteses de correções já estejam contempladas nos processos operacionais.

Deverá ser realizada a regularização imediata de não conformidades relevantes, ou seja, aquelas que comprometam os negócios da HEMERA DTVM.

**Registro e Tratamento de Deficiências**

As deficiências identificadas durante processos de verificação, monitoramento ou auditorias serão registradas em Registro de Deficiências contendo, no mínimo:

- ✓ Eixo ou área afetada;
- ✓ Descrição da lacuna observada;
- ✓ Evidência coletada;
- ✓ Data de identificação;
- ✓ Classificação da criticidade (Alta, Média, Baixa);
- ✓ Responsável designado para correção;
- ✓ Prazo de correção.

Os prazos máximos para correção serão: Alta – até 30 dias corridos; Média – até 60 dias corridos; Baixa – até 90 dias corridos. Deficiências classificadas como de alta criticidade serão comunicadas formalmente à Diretoria Executiva no prazo de até 5 dias úteis a contar da identificação. Após o prazo

estipulado, a área de Compliance e Controles Internos realizará nova verificação para confirmar a implementação da medida corretiva, mantendo registro histórico das ações por, no mínimo, 5 anos.

A HEMERA DTVM admite a concessão de prazos excepcionais para a correção de deficiências que envolvam maior complexidade técnica ou dependência externa, desde que exista justificativa formal e aprovação prévia da área de Compliance.

**Métricas e Indicadores de Conformidade**

1. Percentual de Controles Atualizados

(Controles revisados nos últimos 12 meses / Total de controles mapeados) × 100

Meta: ≥ 90%

observação: riscos altos e muito alto

2. Prazo Médio de Regularização

soma dos dias para correção / nº de correções concluídas

Meta: ≤ 30 dias

3. Testes de Controles Internos

Falha em testes de controles internos nos últimos 12 meses / Total de testes realizados nos últimos 12 meses
Meta: 5%

**Monitoramento de Operações**

Cabe a área de *compliance* e controles internos realizar o monitoramento da distribuição dos negócios e das operações realizadas por meio de verificação de e-mail, gravações ou boletas, para avaliar se observam os critérios descritos nas regras e parâmetros:

- ✓ Confirmação dos tipos de operações aceitas;
- ✓ Conferência do horário das negociações e fechamento das operações;
- ✓ Registro no sistema;
- ✓ No caso de boleta física a validação do cancelamento ou de alterações de operações.

A evidência de não conformidades, os procedimentos para sua solução e aprovação/ciência serão formalizados no sistema.

As ocorrências que causarem impacto de relevância serão objeto de avaliação nas reuniões periódicas da diretoria.

**Planos de Ação**

Identificadas as deficiências e/ou não conformidades e decidida pela investigação das causas e tratamento de soluções alternativas, a área de *compliance* e controles internos avalia a solução que foi adotada de imediato e define se o assunto exige uma ação imediata do gestor responsável.

São adotadas providências sempre que forem detectadas deficiências na execução dos processos operacionais, recebidas reclamações de clientes consideradas procedentes e quando registradas no relatório anual da área de *compliance* e controles internos.

Ação definida por gestores, com indicação de responsáveis e prazo para implementação, visando melhorar processos, minimizar riscos ou solucionar problemas identificados nas autoavaliações das áreas podem ser criados a qualquer momento e decorrentes de qualquer uma das ações-chave relacionadas anteriormente.

A função de conformidade toma conhecimento da ocorrência e das providências adotadas, na medida de sua urgência e da necessidade de tratar a respectiva causa. Caso haja reincidências, comunica imediatamente o gestor responsável e à Diretoria Executiva.

Anualmente a área de *compliance* e controles internos efetua uma análise, em relação às ocorrências reportadas, levando em consideração:

- ✓ Existência de reincidências, tornando-se, portanto, uma deficiência sistêmica;

✓ Probabilidade de voltar a ocorrer.

**Canal de Ética**

Para assegurar o processo de comunicação interna sobre atos de descumprimento ao estabelecido no Código de Ética e Conduta e nas demais políticas, manuais e documentos internos aplicáveis, a HEMERA DTVM dispõe de canal de denúncias para a apuração de questões de não conformidades éticas e ilicitudes de qualquer natureza.

Todos os envolvidos no tratamento das informações têm o dever de manter o sigilo sobre o conteúdo das comunicações recebidas, o andamento do processo e, principalmente, sobre a identidade do denunciante, de forma a preservar sua integridade e garantir a confidencialidade das informações. Caso o denunciante prefira, ele poderá realizar a manifestação de forma anônima, sem a necessidade de identificação.

Os meios de acesso ao canal serão divulgados no ambiente físico da instituição, por meio de comunicações acessíveis a todos os colaboradores, bem como na intranet ou em meio equivalente. Além disso, poderá ser utilizada a área de denúncias do site institucional, assegurando amplo acesso. Ressaltamos que este canal de acolhimento de comunicações, que é de responsabilidade da área de *compliance* e controles internos, também será utilizado para a comunicação de indícios de ilicitude conforme situações e ocorrências descritas no parágrafo único do Artigo 1º. da Resolução CMN nº. 4.859/2020, que possam afetar a reputação dos integrantes do grupo de administradores que detenham o controle bem como, dos membros da Diretoria Executiva.

A área de *compliance* e controles internos participa das reuniões do Comitê de *Compliance* e Riscos, que avalia todos os relatos realizados relativos aos Administradores, Colaboradores, bem como, na supervisão, de terceiros (fornecedores, prestadores de serviço, agentes intermediários, etc.).

Deverão participar do Comitê de *Compliance* e Riscos, além do responsável pela área de *compliance* e controles internos e dos Colaboradores indicados no Código de Ética e Conduta, também responsável pela área competente para tratamento da situação. Caberá aos integrantes do Comitê de *Compliance* e Riscos manterem confidencialidade, independência, imparcialidade e isenção para a avaliação das situações e ocorrências avaliadas.

Após a avaliação do Comitê de *Compliance* e Riscos decisão sobre a comunicação ou não, a área de *compliance* e controles internos será responsável, dentro da estrutura organizacional da HEMERA DTVM, pela comunicação de caso de indícios confirmados ao Banco Central do Brasil. Esta comunicação deverá ocorrer em até dez dias úteis, contados a partir do conhecimento ou do acesso à informação.

A área de *compliance* e controles Internos divulgará em sua página na internet, regulamento que descreva os procedimentos de utilização deste Canal de Ética.

Caberá ainda à área de *compliance* e controles internos elaborar relatório semestral (datas-bases de 30 de junho e 31 de dezembro), contendo, o número de comunicações recebidas, informações sobre as situações e ocorrências comunicadas ao Banco Central, os responsáveis pelo tratamento das situações e ocorrências, prazo médio de avaliação e medidas adotadas para a solução das situações e ocorrências dentro da HEMERA DTVM. O relatório semestral será aprovado pelo diretor responsável pelas áreas de *compliance* e controles internos da HEMERA DTVM e mantido à disposição do Banco Central do Brasil pelo prazo mínimo de cinco anos.

**Relatório Anual de Gestão de Risco de Conformidade**

De acordo com a Resolução BCB n° 65/2021, a área de *compliance* e controles internos elabora, o relatório da função de conformidade com sumário dos resultados das atividades realizadas no exercício encerrado, relatando o trabalho realizado no ano anterior.

O relatório contempla o sumário das atividades, conclusões, recomendações e medidas corretivas adotadas para a mitigação das não conformidades.

**Relatório de Controles Internos**

A área de *compliance* e controles internos deve elaborar o Relatório de Controles Internos de avaliação da qualidade e adequação do sistema de controles internos, que contempla os aspectos necessários ao trabalho de auditoria independente. O Relatório deve ser emitido de acordo com a **Resolução BCB n° 260/2022**, considerando também:

- ✓ Quais as políticas e procedimentos adotados para assegurar a segregação de atividades;
- ✓ Quais as políticas de autorizações específicas e gerais;
- ✓ Processos realizados para a revisão e conciliação contábil;
- ✓ Procedimentos de controle adotados relativos ao gerenciamento de riscos, incluindo identificação e quantificação, reconciliação de posições, estabelecimento e controle de limites de exposição e elaboração de relatórios de posições detidas pela instituição;
- ✓ Descrição dos aspectos relativos à segurança física;
- ✓ Descrição do estabelecimento dos planos de contingência ou de continuidade;
- ✓ Controles para prevenir práticas em atividades indevidas ou ilícitas e para identificar, para não transacionar/bloquear relacionamento e comunicar ao COAF - BACEN, as atividades de lavagem de dinheiro e de financiamento ao terrorismo.

Ademais, o relatório abarcará as questões endereçadas no artigo 25 da Resolução CVM nº 21, de 25 de fevereiro de 2021, conforme alterada. O relatório ficará disponível para a CVM, Banco Central do Brasil e demais órgãos reguladores ou autorreguladores.

**Armazenamento de Documentos**

Toda documentação de clientes é enviada e recebida em sistema, mantida em local adequado e segregado. A documentação permanece arquivada pelo prazo mínimo de 10 (dez) anos. Somente as áreas de cadastro, de *compliance* e controles internos possuem acesso para realizar consultas às documentações, a qualquer tempo.

**Treinamento**

O treinamento tem como objetivo capacitar os Colaboradores, de forma a torná-los aptos a seguir todas as regras dispostas nas políticas internas, manuais e documentos internos da HEMERA DTVM. Todos os Colaboradores receberam o devido treinamento acerca de todas as políticas, manuais, documentos e procedimentos. Assim, serão proporcionados aos Colaboradores uma visão geral das políticas, manuais e

documentos internos da HEMERA DTVM, de forma que eles se tornem aptos a exercer suas funções aplicando conjuntamente todas as normas nelas dispostas.

Ainda, com o intuito de promover o constante aperfeiçoamento dos profissionais da HEMERA DTVM e a melhoria constante das funções dos Colaboradores, cursos de atualização que sejam relacionados às atividades desenvolvidas são incentivados e poderão ser parcialmente patrocinados pela HEMERA DTVM.

Poderão ser ministradas a todos os Colaboradores da HEMERA DTVM palestras internas, a fim de dar ciência sobre (i) as políticas adotadas pela HEMERA DTVM; (ii) a regulamentação vigente e aplicável aos negócios da HEMERA DTVM e, ainda, (iii) eventuais fragilidades detectadas, sobretudo para alertar e evitar práticas que possam ferir a regulamentação vigente no exercício das atividades desenvolvidas pela instituição. Referidas palestras serão de participação obrigatória, comprovada mediante assinatura do Colaborador em lista de presença. Não sendo possível a participação do Colaborador, sua ausência deverá ser justificada ao diretor responsável pela área de *compliance* e controles internos, sendo certo que a ausência deverá ser reposta na data mais próxima possível.

Todo o treinamento interno proposto pela HEMERA DTVM, além de enfatizar a observância das regras e da relação fiduciária com os clientes, terá como objetivo abordar os procedimentos operacionais, especialmente no que diz respeito às informações de natureza confidencial e adoção de posturas éticas e em conformidade com os padrões estabelecidos.

Os treinamentos relacionados ao conteúdo das políticas, manuais e documentos internos da instituição serão realizados com periodicidade mínima anual, pelo diretor responsável pela área de *compliance* e controles internos sendo obrigatórios a todos os Colaboradores e controlados por lista de presença. Quando do ingresso de um novo Colaborador, o diretor responsável pela área de *compliance* e controles internos ou gestor por este designado, aplicará o devido treinamento de forma individual para o novo Colaborador. O referido diretor ou gestor designado poderá, ainda, conforme achar necessário, promover treinamentos esporádicos visando manter os Colaboradores constantemente atualizados em relação às políticas, manuais e documentos internos.

**Recrutamento e Seleção**

A contratação de futuros Colaboradores pela HEMERA DTVM considerará a qualificação adequada para cada posição a ser ocupada, e avaliará não somente a formação técnica dos candidatos, mas também suas experiências em trabalhos anteriores.

Não serão admitidas na HEMERA DTVM as práticas de discriminação, perseguição ou represálias por motivos de idade, origem étnica, cor, religião, sexo, gravidez, nacionalidade, cidadania, opção sexual, deficiência física, estado civil, características genéticas de uma pessoa ou qualquer outra característica protegida por lei.

Especificamente para os Colaboradores responsáveis finais pela distribuição das cotas dos fundos administrados fiduciariamente pela HEMERA DTVM, a contratação do futuro Colaborador pela HEMERA DTVM estará condicionada à devida certificação do Colaborador, concedida pela ANBIMA, conforme detalhado na seção "Política de Certificação" adiante.

**Política de Certificação**

A HEMERA DTVM aderiu e está sujeita às disposições das Regras e Procedimentos de Certificação ANBIMA ("Regras e Procedimentos de Certificação"), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

**Atividades Elegíveis e Critérios de Identificação**

Tendo em vista a atuação da HEMERA DTVM como distribuidora dos seus próprios fundos de investimento, a HEMERA DTVM identificou, segundo as Regras e Procedimentos de Certificação, que o CPA-20 é a única certificação pertinente às suas atividades, aplicável aos profissionais que realizem a distribuição dos fundos de investimento diretamente junto a investidores.

Nesse sentido, a instituição definiu que apenas os Colaboradores com poderes para realizar a distribuição dos fundos de investimento diretamente junto a investidores é elegível ao CPA-20.

**Identificação de Profissionais Certificados e Atualização do Banco de Dados da ANBIMA**

Antes da contratação ou admissão de qualquer Colaborador, a área de *compliance* e controles internos deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação.

O responsável pela área de distribuição deverá esclarecer à área de *compliance* e controles internos se os Colaboradores que integrarão os departamentos técnicos realizarão a distribuição dos fundos de investimento diretamente junto a investidores.

Caso seja identificada a necessidade de certificação, a área de *compliance* e controles internos deverá solicitar a comprovação da certificação pertinente ou sua dispensa concedida pela diretoria da ANBIMA, se aplicável, anteriormente ao ingresso do novo Colaborador.

A área de *compliance* e controles internos também deverá checar se os Colaboradores que estejam se desligando da HEMERA DTVM estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à instituição.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer até o último dia útil do mês subsequente à data do evento que deu causa a atualização, nos termos do Art. 10, §1º, I das Regras e Procedimentos de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pela área de *compliance* e controles internos, liderada por seu respectivo diretor, conforme disposto abaixo.

**Rotinas de Verificação**

Anualmente a área de *compliance* e controles internos deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados.

Colaboradores que não tenham CPA-20 estão impedidos de realizar a distribuição dos fundos de investimento diretamente junto a investidores.

Ademais, no curso das atividades de fiscalização desempenhadas pela área de *compliance* e controles internos, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, o diretor responsável pela área de *compliance* e controles internos poderá declarar de imediato o afastamento do Colaborador, devendo tal diretor, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de solução.

Sem prejuízo do disposto acima, anualmente deverão ser discutidos e revisados os procedimentos e rotinas de verificação para cumprimento das Regras e Procedimentos de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de *compliance*.

**Processo de Afastamento**

Todos os profissionais em processo de certificação, e para os quais a certificação seja, de fato, exigível, poderão ser afastados da distribuição de cotas de fundos de investimento sob administração fiduciária até que se certifiquem.

Aos profissionais já certificados, caso deixem de ser Colaboradores da HEMERA DTVM, deverão assinar documentação pertinente comprovando o afastamento da HEMERA DTVM, bem como os profissionais em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

Os profissionais já certificados que deixarem de ser colaboradores deverão assinar o Termo de Afastamento, conforme modelo constante do Anexo ao presente documento, comprovando o efetivo afastamento da HEMERA DTVM. Igualmente, deverão assinar o referido documento os profissionais em processo de certificação que forem afastados por qualquer dos motivos mencionados nesta seção.

**Verificação e Atualização**

- ✓ Esta política será revisada a cada 12 (doze) meses, ou sempre que houver alterações relevantes, seguindo o mesmo fluxo de aprovação e divulgação estabelecido para sua versão original.

- ✓ A área de Compliance é responsável por coordenar o processo de revisão, promover as atualizações necessárias e assegurar sua adequada divulgação a todos os públicos de interesse.

**Controle de versão**

O controle de versão deste documento, incluindo a identificação dos responsáveis pela sua elaboração, revisão e aprovação, encontra-se disponível no sistema gerencial de Compliance, garantindo rastreabilidade, transparência e adequada governança do processo.

## ANEXO I - Estrutura de Acompanhamento e Monitoramento de Controles Internos

A verificação será realizada nos seguintes eixos:

- ✓ Política de Segurança Cibernética
- ✓ Plano de Ação e Resposta a Incidentes
- ✓ Contratação de Serviços Relevantes e Computação em Nuvem
- ✓ Continuidade de Negócios e Gerenciamento de Riscos

### Eixo 1 – Política de Segurança Cibernética

Confirmar que a política da instituição contempla todos os requisitos normativos, está formalmente aprovada e é revisada periodicamente.

| Item | O que avaliar | Como avaliar | Evidência aceitável |
|---|---|---|---|
| Objetivos de Segurança Cibernética | Se os objetivos incluem prevenção, detecção e redução de vulnerabilidades | Ler seção de objetivos e verificar clareza e abrangência | Trecho da política com a lista de objetivos |
| Procedimentos de Segurança | Se estão descritos autenticação, criptografia, prevenção/detecção de intrusão, prevenção de vazamento, testes de vulnerabilidade, proteção contra malware, rastreabilidade, controles de acesso, segmentação de rede, backups | Conferir lista de controles na política | Página ou tabela na política listando os controles |
| Controles de Rastreabilidade | Se há regras para geração, armazenamento e análise de logs | Localizar seção sobre logs e rastreabilidade | Trecho que define padrões de logs |
| Gestão de Incidentes | Se há processo documentado para registro, análise de causa, impacto e controle de efeitos | Ler seção de gestão de incidentes | Parágrafo descrevendo etapas de gestão de incidentes |

| | | | |
|---|---|---|---|
| Diretrizes para Cenários de Incidentes | Se há definição de cenários de indisponibilidade para testes de continuidade | Conferir seção sobre continuidade | Lista ou tabela com cenários |
| Requisitos para Prestadores | Se define procedimentos e controles exigidos de terceiros que tratem dados sensíveis | Ler seção sobre terceiros | Trecho da política com requisitos para prestadores |
| Classificação de Dados | Se há critérios para classificar dados quanto à relevância | Conferir anexo ou seção de classificação | Matriz de classificação documentada |
| Parâmetros para Avaliação de Incidentes | Se define parâmetros objetivos para relevância de incidentes | Conferir tabela ou lista de parâmetros | Documento ou seção com parâmetros |
| Cultura de Segurança | Se há programas de capacitação, avaliação periódica e comunicação a clientes | Ler seção de cultura de segurança | Plano anual de treinamentos anexado à política |
| Compartilhamento de Informações | Se há processo para compartilhar dados de incidentes com outras instituições | Ler seção sobre compartilhamento | Trecho que descreve fluxo de compartilhamento |

**Eixo 2 – Plano de Ação e Resposta a Incidentes**

Objetivo: Confirmar que o plano contempla todas as ações, rotinas e responsabilidades exigidas, alinhadas à política de segurança da informação.

| Item | O que avaliar | Como avaliar | Evidência aceitável |
|---|---|---|---|
| Ações Estruturais | Se o plano descreve ajustes organizacionais e operacionais para cumprir a política | Ler seção de ações estratégicas | Trecho descrevendo adaptações estruturais |
| Rotinas e Controles | Se há descrição de todas as rotinas, procedimentos e tecnologias para prevenção e resposta | Ler capítulo de procedimentos operacionais | Lista ou tabela com rotinas e tecnologias |

| | | | |
|---|---|---|---|
| Área Responsável | Se define claramente a área responsável pelo registro e controle dos efeitos dos incidentes | Conferir organograma ou seção de responsabilidades | Trecho que nomeia a área responsável |
| Diretor Responsável | Se há designação formal de diretor encarregado do plano | Solicitar termo de nomeação ou ata | Documento de nomeação |
| Relatório Anual | Se o plano prevê e elabora o relatório anual com efetividade das ações, resumo de resultados, lista de incidentes e testes de continuidade | Ler seção sobre relatórios, checar existência do relatório e avaliar conforme requisitos da resolução | Trecho que descreve o relatório anual e evidência da sua existência |

**Eixo 3 – Contratação de Serviços Relevantes e Nuvem**

Objetivo: Confirmar que a instituição documenta a avaliação de prestadores e mantém contratos com cláusulas obrigatórias.

| Item | O que avaliar | Como avaliar | Evidência aceitável |
|---|---|---|---|
| Procedimento de Contratação | Se há documento descrevendo governança, avaliação de capacidade e critérios de risco | Solicitar e ler o procedimento | Procedimento aprovado |
| Avaliação de Capacidade do Prestador | Se contempla cumprimento de legislação, acesso a dados, confidencialidade, integridade, disponibilidade, certificações, auditorias, segregação de dados, controles de acesso | Conferir checklist de due diligence | Formulário de avaliação preenchido |
| Serviços no Exterior | Se há documentação sobre requisitos | Conferir seção ou documento anexo | Documento com requisitos para serviços no exterior |

| | | | |
|---|---|---|---|
| | legais e acesso a dados no exterior | | |
| Cláusulas Contratuais | Se contratos incluem todos os requisitos obrigatórios (países, medidas de segurança, segregação, obrigações na rescisão, acesso a informações, notificações, acesso do BCB) | Revisar amostra de contratos | Cópia de contrato com cláusulas marcadas |

**Eixo 4 – Continuidade de Negócios e Gerenciamento de Riscos**

Objetivo: Confirmar que planos e políticas de continuidade incluem tratamento para incidentes cibernéticos e interrupção de serviços críticos.

| Item | O que avaliar | Como avaliar | Evidência aceitável |
|---|---|---|---|
| Tratamento de Incidentes Cibernéticos | Se políticas e planos preveem ações para mitigar incidentes | Ler seção de incidentes | Trecho com ações documentadas |
| Procedimentos para Interrupção de Serviços | Se há processo para substituição de fornecedor e retomada de operações | Ler capítulo de contingência | Fluxograma ou texto do procedimento |
| Cenários de Teste | Se há lista de cenários de indisponibilidade considerados nos testes | Ler plano de testes | Lista de cenários documentados |
| Prazos para retomada | Se define prazos para normalização de serviços | Ler seção de RTO/RPO | Quadro com prazos |
| Critérios de Crise | Se há critérios documentados para definir situação de crise | Ler seção de definição de crise | Lista de critérios |
| Comunicação a Autoridades | Se há procedimento para notificação de | Ler capítulo de comunicação | Texto com fluxo de notificação |

| | | | |
|---|---|---|---|
| | incidentes e medidas adotadas | | |