Política de Controles Internos

SUMÁRIO

1. OBJETIVO 2
2. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO 2
3. DEFINIÇÕES 2
4. ESTRUTURA DE CONTROLES INTERNOS 2
4.1 PROCESSO DE IDENTIFICAÇÃO, CLASSIFICAÇÃO E TRATAMENTO DOS RISCOS 3
4.2 DISSEMINAÇÃO DE CULTURA DE RISCOS 3
4.3 PROGRAMAS DE TREINAMENTO 3
4.4 SEGREGAÇÃO DE FUNÇÕES 4
4.5 CANAIS DE COMUNICAÇÃO 4
4.6 SEGURANÇA PARA OS SISTEMAS DE INFORMAÇÃO 4
5. DIRETRIZES 4
6. RESPONSABILIDADES 5
6.1 COLABORADORES 5
6.2 GESTÃO DE RISCOS OPERACIONAIS 6
6.3 COMPLIANCE 7
6.4 AUDITORIA INTERNA 7
6.5 JURÍDICO 8
7. TESTE DE CONTROLES INTERNOS 8
7.1 TESTES DOS CONTROLES 8
7.2 TESTES DE CONTROLES MANUAIS 8
7.3 TESTES DE CONTROLES AUTOMÁTICOS 10
7.4 TESTES DE CONTROLES EVENTUAIS - POR DEMANDA/EVENTO 10
8. RELATÓRIO DE CONTROLES INTERNOS 11

1. OBJETIVO

Em atendimento à Resolução n° 4.968/21, do Conselho Monetário Nacional ("CMN"), Circular n° 3.978/20 do Banco Central do Brasil ("BACEN"), as Resoluções n° 21/21, 30/21, 32/21, 35/21 e 50/21 da Comissão de Valores Mobiliários ("CVM"), à Circular n° 612/20, à Resolução 416 da Superintendência de Seguros Privados ("SUSEP") e à regulamentação Rule and Statement of Guidance, Internal Controls for Regulated Entities da Cayman Islands Monetary Authority ("CIMA"), a Lei Sarbanes-Oxley (SOx) da Securities and Exchange Commission ("SEC") e aderência às melhores práticas de mercado, o Grupo XP Inc. ("Grupo") estabelece, por meio da Política de Controles Internos ("Política"), as diretrizes e responsabilidades a serem atendidas para o fortalecimento do seu ambiente de controles internos.

2. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

Esta Política entra em vigor a partir da data de sua publicação e deve ser revisada e aprovada pela Diretoria. Se, no decorrer do período, houver mudança relevante no ambiente regulatório ou na estrutura de controles internos, o documento deverá contemplar a alteração.

Esta política deverá ser amplamente divulgada dentro do Grupo e disponibilizada a todos os colaboradores através da Intranet da XP.

3. DEFINIÇÕES

Grupo XP Inc.: Empresas Controladas pela XP Inc. e suas Coligadas, constituídas no Brasil e no Exterior, consideradas em conjunto.

Coligadas: As sociedades em que a XP Inc. tenha influência significativa (art. 243, §1º, da Lei nº 6.404/76).

Controladas: As sociedades nas quais a XP Inc. é Acionista Controladora.

Acionista Controlador: O acionista ou grupo de acionistas que controlam a Companhia e suas Coligadas, vinculado(s) por acordo de voto ou sob controle comum, que exerça(m) o poder de controle, direto ou indireto, sobre sociedade, nos termos da Lei nº 6.404/76.

Conglomerado Prudencial XP: a XP Investimentos CCTVM S.A., Banco XP S.A., a XP Serviços Financeiros DTVM Ltda. e demais empresas do Grupo XP Inc., constituídas no Brasil e no Exterior, que se enquadram na definição que consta da Resolução n° 4.950/21, do CMN.

4. ESTRUTURA DE CONTROLES INTERNOS

A estrutura de controles internos é parte integrante da estrutura de governança do Grupo, e busca assegurar a existência de um processo efetivo de identificação e avaliação dos riscos por meio de análise e monitoramento dos controles existentes.

O Grupo adota o modelo das 3 linhas de defesa que estão envolvidas no alinhamento das normas internas com o ambiente de controle necessário para prevenir e combater qualquer ato de natureza ilícita, bem como assegurar que os principais riscos envolvidos nas operações do Grupo sejam conhecidos, monitorados e tratados adequadamente:

i. **Primeira linha:** Representada pelas áreas de negócios e de suporte para suas atividades que gerem a exposição de riscos, de acordo com as políticas, o apetite de riscos (RAS) e outras condições aprovados

pela Diretoria do Grupo. A primeira linha deve ter meios para identificar, mensurar, gerenciar e reportar os riscos assumidos.

ii. **Segunda linha:** Representada pelas áreas de controle que atuam na revisão independente das atividades, processos e controles realizados pela Primeira Linha, em linha com o Apetite de Riscos do Grupo. Responsável pela proposição de políticas de gestão de riscos, metodologias de riscos e por supervisionar a supervisão da Primeira linha.

iii. **Terceira linha:** Representada pela auditoria interna que é responsável por assegurar, de forma independente e sem conflito de interesses, à Diretoria Estatutária e ao Comitê de Auditoria a adequação do ambiente e da estrutura de riscos do Grupo, incluindo as atividades da primeira e da segunda linha.

Outros elementos importantes da estrutura de gerenciamento de risco do Grupo é a estrutura executiva, de comitês e fóruns técnicos.

As atividades de controles devem ser constantemente avaliadas, tomando como referência as boas práticas estabelecidas pelos padrões do *Committee of Sponsoring Organization of Tradeway Commission* – COSO.

A estrutura de controles internos tem como objetivo:

4.1 PROCESSO DE IDENTIFICAÇÃO, CLASSIFICAÇÃO E TRATAMENTO DOS RISCOS

Os trabalhos de controles internos consistem em mapeamento de processos, controles, bem como avaliação de sua efetividade para mitigação dos riscos. Esse processo visa garantir que a estrutura de controles internos conduza à compreensão dos principais riscos decorrentes das atividades e operações do Grupo e que potenciais deficiências identificadas sejam corrigidas.

4.2 DISSEMINAÇÃO DE CULTURA DE RISCOS

Com o objetivo de manter altos padrões de integridade e valores éticos e buscando a participação de todos seus colaboradores no processo de controles internos, o Grupo atua para estabelecer, manter e aprimorar uma cultura de entendimento e proatividade no que tange aos processos de controles internos.

Em linha com esses objetivos, a área de gestão de riscos corporativos é responsável pela disseminação periódica da cultura do risco através das diferentes áreas do Grupo. A responsabilidade principal é assegurar que todos participem dos valores da cultura de governança e que tenham conhecimento, de forma clara, dos papéis e responsabilidades no sistema de controles internos e prevenção de riscos.

4.3 PROGRAMAS DE TREINAMENTO

Para desempenhar satisfatoriamente os seus negócios e cumprir exigências regulamentares, o Grupo assegura que todos os colaboradores recebam sessões de treinamento e atualização, com a periodicidade estabelecida pela estrutura de controle do Grupo, de modo que todos tenham conhecimento das normais políticas e regulamentações vigentes aplicadas ao Grupo. Os treinamentos aplicados abordam os temas:

- Programa de Compliance, incluindo Código de Ética, diretrizes sobre investimentos pessoais, anticorrupção, brindes, presentes e hospitalidades, bem como orientações sobre circulação de informações e riscos reputacionais;

- PLD/FT – Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, incluindo prevenção a fraudes, utilização do canal confidencial e responsabilidades individuais;
- Suitability, com foco na adequação de produtos, serviços e operações ao perfil do cliente;
- Gestão de Riscos Corporativos, abrangendo gerenciamento de riscos, coordenação de novos produtos e negócios (TAC & NAC), continuidade de negócios e observância às políticas corporativas;
- Segurança da Informação, incluindo proteção de dados, boas práticas de segurança cibernética e uso responsável de inteligência artificial;
- Temas transversais de Diversidade e Segurança e Saúde do Trabalho, reforçando a cultura ética, o ambiente corporativo seguro e inclusivo.

4.4 SEGREGAÇÃO DE FUNÇÕES

Implementar controles que monitorem a execução das atividades é essencial para garantir a segurança das informações e impedir a ocorrência de fraudes e erros. Desta forma, a Grupo adotam diretriz de segregação de funções que prevê que cada atividade operacional deverá ser exercida por 2 (dois) ou mais colaboradores, sendo cada um deles responsável, separadamente, pela execução e aprovação/autorização do procedimento.

A respectiva diretriz de segregação de funções minimiza o risco operacional a que o Grupo está exposto, uma vez que não permite que ocorram relações baseadas meramente em confiança ou amparadas em interesses próprios, bem como inibe que procedimentos sejam realizados sem a devida revisão.

Cabe destacar que, para a correta aplicação da política de segregação de funções, todos os Colaboradores têm seus acessos físicos e lógicos restritos às funções e às atividades exercidas.

4.5 CANAIS DE COMUNICAÇÃO

Nos termos do art. 5º, inciso IV, alínea a da Resolução nº 4.968/21, do CMN, os controles internos devem prever a existência de canais de comunicação que assegurem aos funcionários, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades.

A instituição disponibiliza em sua Intranet as suas políticas e procedimentos com as diretrizes a serem seguidas por seus funcionários.

4.6 SEGURANÇA PARA OS SISTEMAS DE INFORMAÇÃO

Os sistemas necessários para suportar a realização da prestação dos serviços do Grupo estão sob o ambiente de controle da área de Segurança da Informação, a área visa garantir a proteção e a manutenção da integridade, confidencialidade e disponibilidade das informações de sua propriedade e/ou sob sua guarda, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pelo Grupo para o alcance dos objetivos de segurança da informação.

5. DIRETRIZES

Essa Política tem como diretrizes:

- Manter altos padrões de integridade e valores éticos, por intermédio da disseminação de cultura de riscos que enfatize e demonstre a todos os colaboradores e envolvidos a importância dos controles internos;
- Assegurar a conformidade com leis e regulamentos aplicáveis emitidos por órgãos supervisores nacionais, visando a transparência e aderência às políticas, normas e procedimentos internos estabelecidos;
- Garantir que a estrutura de controles internos conduza à compreensão dos principais riscos decorrentes de fatores internos e externos incorridos pelo Grupo, com a finalidade de assegurar que sejam identificados, avaliados, monitorados, controlados e testados de forma eficiente e eficaz;
- Assegurar a disponibilidade de canais de informação que assegurem os empregados, a obter acesso a informações confiáveis, tempestivas e compreensíveis consideradas relevantes para suas tarefas e responsabilidades;
- Manter o sistema de controles internos alinhado com as melhores práticas, o qual deverá periodicamente ser revisado e atualizado, a fim de que eventuais deficiências identificadas sejam corrigidas, de forma a garantir sua efetividade, incluindo os processos de identificação e mensuração dos riscos de mercado, crédito e operacional, e validação dos modelos de precificação e testes de estresse;
- Assegurar a existência de atribuição de responsabilidade e de delegação de autoridade, observada a estrutura hierárquica estabelecida pelo Grupo, garantindo a apropriada segregação de funções, de modo a eliminar atribuições de responsabilidades conflitantes, assim como reduzir e monitorar, com a devida independência requerida, potenciais conflitos de interesses existentes nas Áreas;
- Proporcionar a consistência e tempestividade das informações que são relevantes para a tomada de decisões ou que afetem as atividades do Grupo, por meio de processo de comunicação confiável, oportuno, compreensível e acessível ao público externo, funcionários e colaboradores;
- Garantir a elaboração de relatórios, conforme prazos estabelecidos pelos reguladores e autorreguladores, sobre as conclusões e recomendações dos controles internos do Grupo, a serem apreciados alta administração e quando aplicável em fóruns relevantes.
- Implementar procedimentos específicos para identificação e monitoramento de fraudes e corrupção, além de disponibilizar programas de treinamentos e orientações sobre conduta e comunicação de suspeitas de violação ou irregularidades, auditoria interna e avaliação periódica da exposição aos riscos de fraude e corrupção; e
- Assegurar que as demandas, solicitações ou questionamentos gerados pelos reguladores serão atendidos nos prazos estipulados nas regulamentações vigentes aplicáveis ou ofícios gerados.

6. RESPONSABILIDADES

6.1 COLABORADORES

Todos os colaboradores do Grupo devem:

i. Cumprir as regras estipuladas pelos normativos do Grupo e leis que regulamentam a Estrutura de Controles Internos;

ii. Cumprimento do Código de Ética;

iii. Manter um efetivo ambiente de controle relacionado às atividades desenvolvidas, consistente com a natureza, complexidade e risco das operações realizadas;

iv. Definir e implementar os planos de ação para endereçamento dos apontamentos efetuados pelas auditorias internar e externas, reguladores e controles internos;

v. Garantir a aplicação das decisões, políticas e estratégias aprovadas, e a manutenção do ambiente de controle adequado;

vi. Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizada pelo Grupo; e

vii. Comunicar imediatamente à sua liderança e a área de Riscos qualquer descumprimento ou violação à Estrutura de Controles Internos do Grupo, problemas nas operações e violações das políticas da instituição ou de disposições legais e regulamentares.

Diretoria

A Diretoria deve se envolver ativamente na definição de controles internos, mediante:

i. Promoção de elevados padrões éticos e de integridade

ii. estabelecimento de cultura organizacional com ênfase na relevância dos sistemas de controles internos e no engajamento de cada funcionário no processo de controle interno

iii. manutenção de estrutura organizacional adequada para garantir a qualidade e a efetividade dos sistemas e processos de controles internos, incluindo a revisão e aprovação desta Política

iv. garantir de recursos adequados e suficientes para o exercício das atividades relacionadas aos sistemas de controles internos, de forma independente, objetiva e efetiva

v. monitorar a adequação e eficácia dos sistemas de controle interno.

vi. Patrocinar a implantação de práticas de negócio eficientes e controles internos adequados e eficazes;

vii. implementar as diretrizes relativas aos sistemas de controles internos

viii. monitorar a adequação e eficácia dos sistemas de controle interno.

ix. Devem ter ciência e adotar as medidas necessárias acerca das ações a serem implementadas para correção tempestiva das deficiências apontadas nos relatórios semestrais de controle e de gerenciamento do risco operacional.

6.2 GESTÃO DE RISCOS OPERACIONAIS

A área de Gestão de Riscos Corporativos é composta por riscos operacionais, controles internos e continuidade de negócios. Com isso, a área detém uma rotina de identificação, classificação, monitoramento e reporte de riscos alinhado com as expectativas regulatórias e melhores práticas do mercado, de modo a prestar, tempestivamente, à Diretoria uma visão holística dos riscos identificados, seu grau de exposição, a qualidade, efetividade operacional de seus controles, bem como supervisão de planos de mitigação e implementação de controles e processos e metodologias para gestão de continuidade de negócios.

Dessa forma, as principais atribuições da área com relação a controles internos são:

- Efetuar a avaliação periódica do ambiente de controles internos – desenho e efetividade operacional dos controles – por meio de mapeamento dos processos, testes periódicos de efetividade dos controles para uma amostra de eventos e ou em sua totalidade.
- Acompanhar a implementação de planos de ação e medidas corretivas que visem a redução e/ou mitigação dos Riscos Corporativos;
- Propor a diretoria cronograma de trabalhos de controles internos, considerando os escopos regulatórios aos quais o Grupo seja sujeita.
- Elaborar os relatórios e cartas de controles internos, conforme regulamentação aplicável considerando:
  - a avaliação sobre a adequação e a efetividade dos sistemas de controles internos;
  - as recomendações a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento, quando for o caso; e
  - a manifestação dos responsáveis pelas correspondentes áreas a respeito das deficiências encontradas em verificações anteriores e das medidas efetivamente adotadas para saná-las.

A metodologia utilizada na abordagem de riscos e controles internos tem como objetivo estabelecer diretrizes aplicada nos processos de identificação, avaliação do impacto e probabilidade e natureza dos riscos corporativos não financeiros aplicável a todas as empresas do Grupo, independente do seguimento, porte, localização ou forma de atuação. Contempla também as respectivas diretrizes para identificação, formalização e execução dos testes dos controles internos, conforme a sua natureza, relevância e impacto no ambiente de riscos e controles do Grupo, conforme formalizado no documento "Metodologia de Gestão de Riscos e Controles Internos".

6.3 COMPLIANCE

Cabe à área de *Compliance*:

i. Promover uma cultura organizacional que incentive condutas éticas e o compromisso da do Grupo com o cumprimento das regulamentações e leis vigentes, por meio de treinamentos e políticas;

ii. Implementar processos de análise aprofundada de clientes, parceiros e fornecedores, visando o cumprimento das regulamentações de PLDFTP, sanções e risco social, ambiental e climático;

iii. Avaliar previamente os riscos de imagem e regulatório sobre novos produtos/serviços, alterações relevantes em processos, sistemas ou modelo de negócio do Grupo.

iv. Reportar e deliberar no Comitê de PLDFTP casos de alta criticidade e ou mudanças de metodologias.

v. Reportar ao Comitê de Auditoria todas as decisões relevantes de *compliance*.

6.4 AUDITORIA INTERNA

A área de Auditoria Interna deve:

i. Avaliar e testar, de forma independente, os riscos mais relevantes do Grupo, bem como desafiar a completude e acurácia do mapa de riscos corporativos com objetivo de validar se os riscos relevantes estão declarados e monitorados adequadamente;

ii. Avaliar e testar, de forma independente, o desenho e a efetividade dos processos corporativos e controles internos, promovendo a contínua melhoria e aumento do grau de maturidade dos processos;

iii. Avaliar periodicamente os processos relativos ao gerenciamento de riscos e recomendar melhorias do respectivo ambiente de controle interno; e

iv. Avaliar e testar a conformidade com as políticas, normas, procedimentos e regulamentações internas e externas, bem como aderência às recomendações e requisitos dos órgãos de supervisão e resolução dos apontamentos identificados pela própria auditoria interna.

6.5 JURÍDICO

Cabe à área do Jurídico Regulatório, para atendimento ao disposto Norma de Supervisão sobre Controles Internos n° 17/2025, no que tange ao procedimento de manutenção do cadastro do Participante atualizado junto à B3, estabelece-se que a execução do controle como 1ª linha é de responsabilidade da área Jurídica, a qual assegura a atualização tempestiva das informações cadastrais, incluindo, entre outros, a indicação de diretores responsáveis, responsáveis pelas atividades desempenhadas, composição da diretoria e documentação societária pertinente.

Como mecanismo de supervisão, a 2ª linha, representada pela área de Controles Internos, realiza, com periodicidade anual, a verificação independente desse processo, mediante análise de evidências como capturas de tela (prints) dos sistemas de registro, confrontando as informações registradas com a documentação societária vigente, de forma a validar a consistência, completude e aderência às exigências regulatórias aplicáveis.

7. TESTE DE CONTROLES INTERNOS

7.1 TESTES DOS CONTROLES

É a comprovação da efetividade do funcionamento dos controles. os testes possuem critérios diferentes para os controles manuais (dependentes de TI) e para os controles automáticos.

7.2 TESTES DE CONTROLES MANUAIS

Consiste em comprovar de forma amostral que o controle foi efetuado. O tamanho da amostra depende da frequência em que o controle ocorre:

A tabela a seguir ilustra o direcionador para definição dos tamanhos de amostra a serem considerados ao planejar a extensão dos testes sobre frequência/periodicidade dos eventos ocorridos para o período de 01 ano para fins de testes de controles internos SOx:

Frequência do controle	Intervalo da quantidade de ocorrências	Tamanho mínimo da amostra		
		Baixo	Médio	Alto
Anual	1	1		
Semestral	2	1		2
Trimestral	2-4	2		
Mensal	5-12	2 a 5		
Semanal	13-52	6	10	15
Diário	53-250	20	30	40
Múltiplas vezes ao dia	Mais que 250	25	45	60
Por ocorrência/sob demanda	Obter o total de eventos ocorridos (população) e enquadrar no intervalo das frequências acima.			

Tabela 1: Amostra de testes para SOX

A tabela a seguir ilustra o direcionador para definição dos tamanhos de amostra a serem considerados ao planejar a extensão dos testes sobre frequência/periodicidade dos eventos ocorridos para o período de 01 ano para fins de testes de controles internos não contemplados nos processos SOx:

Frequência do controle	Intervalo da quantidade de ocorrências	Tamanho mínimo da amostra
Anual	1	1
Semestral	2	1
Trimestral	2-4	2
Mensal	5-12	3
Semanal	13-52	8
Diário	53-250	20
Múltiplas vezes ao dia	Mais que 250	25
Por ocorrência/sob demanda	Obter o total de eventos ocorridos (população) e enquadrar no intervalo das frequências acima.	

Tabela 2: Amostra de testes para controles internos (não SOX)

Essas amostras levam em conta intervalos estatísticos, de acordo com as taxas de desvio no universo não testado, conforme proposto pelo *American Institute of Certified Public Accountants* (AICPA).

7.3 TESTES DE CONTROLES AUTOMÁTICOS

Consiste em avaliar periodicamente o funcionamento do controle computadorizado. O tamanho da amostra e a frequência do teste podem ser mínimos (1 vez por semestre), uma vez que esses controles serão exercidos exatamente da mesma maneira, até que o programa computacional seja modificado.

7.4 TESTES DE CONTROLES EVENTUAIS - POR DEMANDA/EVENTO

Alguns controles operam de forma sazonal ou não possuem uma frequência específica, ou seja, ocorrem por evento ou demanda, como aqueles sobre alterações de taxa ou manutenção de um sistema, por exemplo. Para estes casos, deve-se avaliar o histórico de ocorrências no último ano, e estimar uma frequência aproximada que fique entre a "Anual" (1 amostra/ano) e "Diária" (40 amostras/ano).

Exemplo: um controle de alteração de taxas que tenha ocorrido 10 vezes no último ano. A frequência a ser estimada é a "Mensal", pois é a frequência que mais se aproxima do histórico do último ano (12 meses para 10 ocorrências). E controle "Mensal" testa-se 4 amostras/ano.

8. RELATÓRIO DE CONTROLES INTERNOS

Em atendimento à legislação vigente, a área de Gestão de Riscos Corporativos elabora, na periodicidade determinada pelo regulador e/ou autorregulador, relatórios de controles internos, com o resultado de testes efetuados para cada controle avaliado, recomendações e o acompanhamento dos planos de ação definidos nos relatórios anteriores.

Os relatórios de controles internos são avaliados e aprovados pelos diretores indicados nos reguladores responsáveis por Controles Internos e encaminhados para a Alta Administração de cada uma das Controladas, para conhecimento dos principais pontos de atenção quanto aos controles que mitigam os riscos da empresa e deliberação para possíveis revisões e mudanças na estrutura de controles internos.