



Relatório Anual Integrado 2024



Fundação
Itaú Unibanco
Previdência Complementar

Gestão de Riscos e Compliance

Gestão de riscos > p. 31

Controles Internos, Riscos Operacionais e demais riscos > p. 35

Segurança da informação > p. 36

Compliance > p. 37

Programa de Cultura de Gestão Baseada em Riscos > p. 38

Auditoria Interna > p. 39



Gestão de Riscos

GRI 2-16 | 3-3

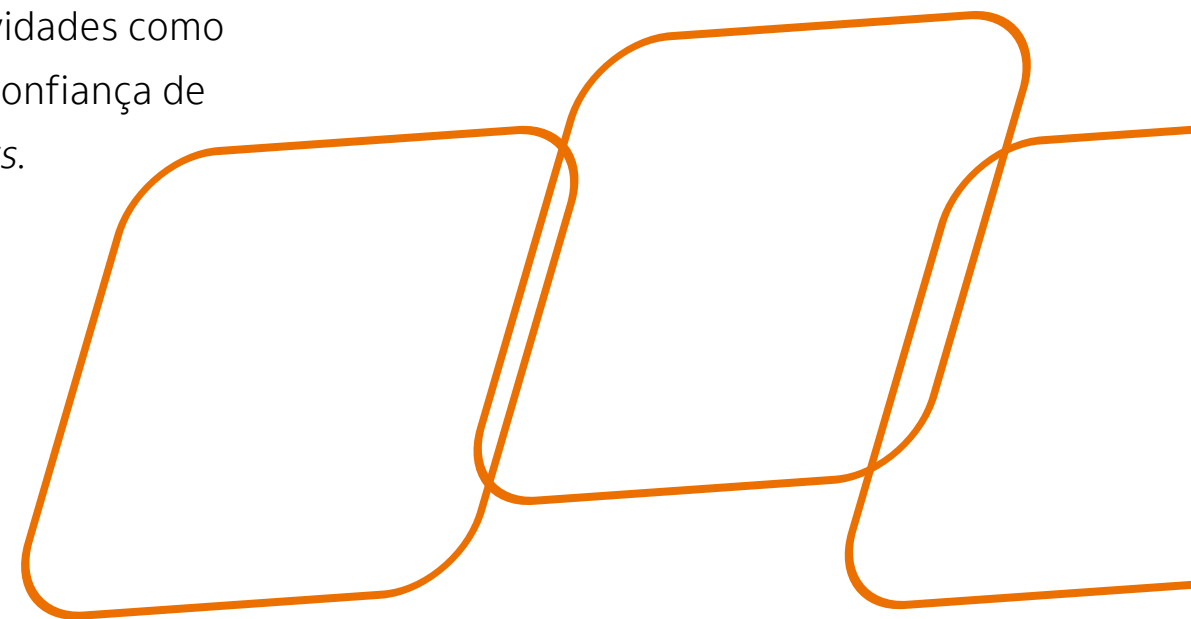
Em 2024, reafirmamos nosso compromisso com a gestão integrada de riscos, por meio de uma atuação robusta de todas as áreas.

Ao longo do ano, fortalecemos as estruturas de controle, o mapeamento e a mitigação de

riscos, além de promovermos uma cultura de gestão baseada em riscos.

Priorizamos a transparência e a comunicação, com o apoio de workshops e treinamentos regulares, garantindo que todos os colaboradores estejam cientes das políticas a serem seguidas.

Nosso compromisso com a gestão integrada de riscos não apenas protege nossas atividades como também reforça a confiança de nossos *stakeholders*.



□□ Em 2024, reafirmamos nosso compromisso com a gestão integrada de riscos, por meio de uma atuação robusta e focada envolvendo todas as áreas. Ao longo do ano, fortalecemos as estruturas de controle, o mapeamento e a mitigação de riscos, além de promovermos uma cultura de gestão baseada em riscos. □□

Ana Silvia Puleghini
Gerente de Compliance
e Controles Internos



Ana Silvia Puleghini fala sobre os destaques das ações!
Acesse o vídeo pelo QRCode ou [link](#)



Modelo de Gestão

GRI 2-13

A alta administração tem o compromisso de guiar a cultura organizacional em conformidade com as diretrizes de gestão integrada de riscos e as melhores práticas do setor, assegurando transparência, governança e garantindo a continuidade das operações em linha com essas diretrizes.

Adotamos o modelo de três linhas de defesa para o gerenciamento dos riscos.

Reportamos periodicamente as ações de mitigação de riscos aos respectivos Comitês de Gestão de Riscos e incluímos nos relatórios gerenciais, já mencionados na [página 25](#) deste relatório.

1ª linha | áreas gestoras das atividades operacionais

Gerencia os riscos nas atividades do dia a dia, sendo responsável por manter um ambiente de controle efetivo nas tarefas desenvolvidas, além de gerenciar os eventos de risco e acompanhar os processos sob sua responsabilidade.

2ª linha | controle de riscos

Apoia as áreas gestoras das atividades operacionais na identificação dos riscos inerentes aos processos, na elaboração e implantação de controles para mitigação de tais riscos, registrando falhas e monitorando sua correção. Também é responsável por disseminar a cultura de riscos e controles, e divulgar as melhores práticas e políticas relacionadas ao gerenciamento integrado de riscos.

3ª linha | auditoria interna

Fornece uma avaliação independente das atividades, contribuindo para a avaliação do nível de maturidade da gestão de riscos.



Mapeamento, monitoramento e controle



Como forma de mitigar os riscos, utilizamos instrumentos normativos, como o regimento dos órgãos estatutários, regulamentos dos planos, políticas e procedimentos internos. Paralelamente, as áreas

gestoras dos processos utilizam controles preventivos e detectivos para monitoramento. Caso ocorra a materialização dos riscos, um apontamento é aberto para registro e tratamento da falha.

A análise sistêmica dos processos garante a transparência e facilita o acompanhamento pelos órgãos estatutários e pelo Comitê de Auditoria. Esses órgãos acompanham e avaliam a gestão de riscos, bem como as medidas de integridade

e ética adotadas, com base em informações fornecidas pela Diretoria Executiva, relatórios gerenciais e pelo Relatório Semestral de Controles Internos emitido pelo Conselho Fiscal, de forma a aumentar a segurança no direcionamento e alcance dos objetivos.

Em 2024, não foram identificados impactos negativos em razão de falhas relacionadas à gestão de riscos ou ao dever fiduciário.

Gestão de Riscos

Controle de riscos

GRI 2-13

Com foco na transparência e prestação de contas das atividades, contamos com Comitês de Gestão, subordinados à Diretoria Executiva, que têm o objetivo de auxiliá-la, através da discussão e avaliação de questões dentro do seu escopo, permitindo que os assuntos a eles relacionados sejam tratados com maior profundidade.

Comitês

Comitê de Controle de Riscos em Investimentos:

monitora os riscos de mercado, crédito e liquidez, apoiando nossos órgãos estatutários na definição de medidas de risco e limites para os diversos segmentos de investimentos. Também monitora o desempenho em relação à tomada de risco e à aderência aos limites legais e políticas de investimentos.

**SAIBA MAIS**

sobre o resultado do monitoramento dos riscos em 2024 na [página de Investimentos](#).



Comitê de Risco Atuarial:

monitora a aderência das premissas biométricas, demográficas, econômicas e financeiras, seus desvios e adequação às características dos participantes e assistidos de cada plano de benefício. Além disso, acompanha os estudos técnicos de convergência da taxa real de juros com base na projeção de retorno e compromissos atuariais.

Comitê de Risco Operacional e Compliance (“CIROC”):

visa o acompanhamento e monitoramento do ambiente de controles, riscos operacionais, demais riscos (compliance, imagem e reputacional, segurança da informação (SI), pessoas, PLD, etc) e adequações regulatórias, envolvendo todos os os nossos processos.

Comitê de Tecnologia, Segurança da Informação e Privacidade de Dados:

visa a preservação e proteção do nosso ambiente tecnológico e de segurança da informação, através do monitoramento dos fornecedores críticos, do acompanhamento dos projetos com dependência de Tecnologia e de indicadores relacionados ao tema. Visa também monitorar, acompanhar e alinhar as regras para a coleta, o armazenamento, tratamento e compartilhamento dos dados pessoais.



Controles Internos, Riscos Operacionais e demais riscos

Em relação aos riscos classificados como operacionais e demais riscos (compliance, imagem e reputacional, SI, pessoas, PLD etc), coordenamos diversas iniciativas visando o aprimoramento dos controles e da gestão dos riscos.

Conheça a seguir as principais ações em 2024:

Gestão do Mapa de Processos e Riscos:

nossa metodologia. envolve a identificação, priorização, resposta, monitoramento e reporte de riscos. Todos os processos são classificados no Mapa de Processos e Riscos, distribuídos em quadrantes de impactos, e a gestão contínua garante a atualização e adequação constante ao ambiente de riscos.

Avaliação de Ambiente de Controle:

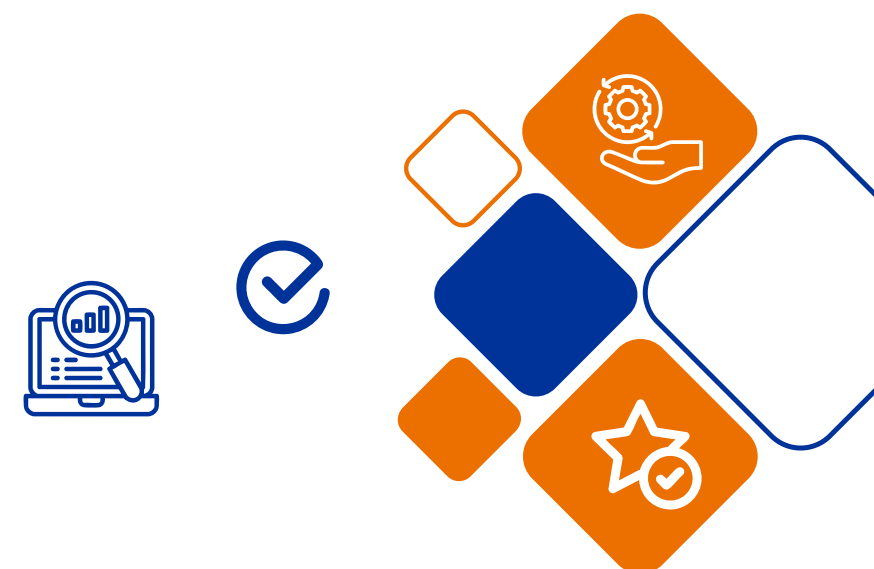
a gestão do Mapa de Processos e Riscos é feita pela avaliação periódica do ambiente de controle de cada processo, que consiste na realização de avaliações e testes, aferindo sua eficácia e obtendo evidências da realização dos controles-chave definidos pela área. Em caso de identificação de inconsistências, é aberto apontamento para tratamento da falha.

Gestão de Ocorrências:

quando uma falha é identificada, abrimos um apontamento de risco levando à definição e implantação de plano de ação para tratamento. Essa resposta é monitorada e reportada a todos os envolvidos através dos boletins mensais, na reunião do Comitê de Controles Internos, Risco Operacional e Compliance (CIROC), e na reunião do Conselho Fiscal para elaboração do relatório semestral.

Demais Monitoramentos de Risco Operacional e Compliance:

monitoramento do atendimento ao prazo das obrigações regulatórias, das auditorias interna e externa, e das demandas dos órgãos fiscalizadores e canais críticos, além do monitoramento da aderência e cumprimento às leis e aos normativos internos e externos.



Segurança da informação

Monitoramento de Risco de Segurança da Informação

Dentre os demais riscos, o risco de Segurança da Informação é cada vez mais frequente. Vivemos em uma época de alta exposição de dados, os tornando um dos recursos mais importantes e valiosos da atualidade.

Realizamos o monitoramento com base em indicadores e considerando a exposição de nossas áreas e fornecedores aos riscos de vazamento de informações, fraudes e ataques cibernéticos.

Essas ações refletem o cuidado diário e contribuem para a nossa segurança. Conheça os indicadores utilizados no monitoramento:

Teste de Intrusão (Pentest):

utilizado para verificar a existência de vulnerabilidades sob a ótica de um atacante motivado e tecnicamente capaz.

No teste realizado em 2024 em fornecedor de sistema crítico, foram identificadas 05 vulnerabilidades (níveis alto, baixo e informativo). Após as correções efetuadas pelo fornecedor, será realizado novo teste a fim de evidenciar as adequações realizadas.

Relatório Security Scorecard:

utilizado no controle de 06 fornecedores de sistemas, o relatório consolida 10 indicadores que monitoram o ambiente de controle dos endereços de IP/URL's dos nossos fornecedores de sistemas.

No fechamento de 2024, tivemos 1 fornecedor com nota A, 03 com nota B, 01 com nota C e 01 com nota F. O nível de risco é levado em consideração na continuidade do contrato com o fornecedor.

Avaliações de Fornecedores e Ferramentas:

o processo tem como objetivo avaliar os mecanismos de segurança do fornecedor e a ferramenta a ser contratada e utilizada.

Em 2024, 11 fornecedores passaram pela avaliação.

Scan de Vulnerabilidades:

software utilizado para avaliação de vulnerabilidades dos sites e URL's de 05 fornecedores.

Em 2024, foi identificada 01 vulnerabilidade de nível baixo, corrigida pelo fornecedor, além de casos falso-positivos.



Compliance

Operamos de maneira ética e responsável sendo o Compliance um componente essencial de nossa gestão integrada de riscos. Nossas ações buscam fazer cumprir normas externas e internas aplicáveis às atividades, bem como evitar, detectar e tratar quaisquer desvios que venham a ocorrer. Conheça a seguir as principais ações em 2024:

Políticas e Procedimentos

Atualmente contamos com 43 normativos internos, divididos nos temas:

- Gestão de Risco
- Integridade e Ética
- Governança
- Pessoas
- Contábil
- Controle Financeiro
- Comunicação
- Investimentos
- Jurídico

Em 2024, todas as áreas se dedicaram à revisão dos normativos internos, visando manter as diretrizes a serem seguidas sempre atualizadas.

Análise Normativa

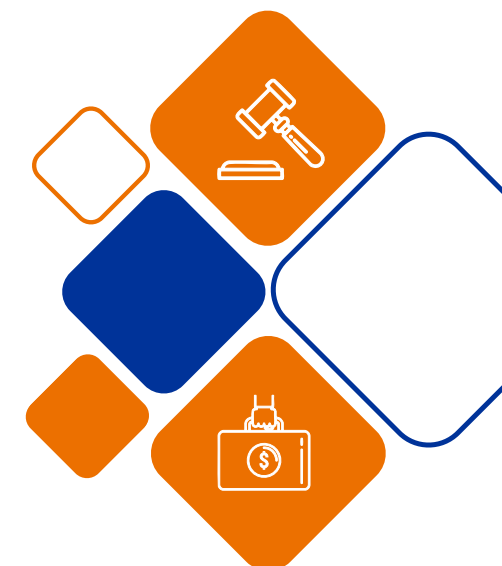
Monitoramos as normas, analisamos seu impacto e conformidade e, quando necessário, abrimos um apontamento para acompanhar sua adequação. Em 2024, avaliamos 179 normativos, 89% analisados como aderentes e/ou sem impacto.

Prevenção à Lavagem de Dinheiro (PLD/CFT)

Em 2024, atualizamos e publicamos o relatório de efetividade dos controles relacionados ao tema.

Programa de Integridade e Ética

Monitoramos também o cumprimento do Programa de Integridade e Ética, o qual abordaremos mais adiante.



Além da gestão dos normativos internos e da análise normativa, estabelecemos em conjunto com as áreas uma série de controles de monitoramento para garantir o cumprimento normativo, fortalecendo assim a gestão e mitigação dos riscos:

- **Obrigações regulatórias** | 26 obrigações cadastradas em sistema. Todas atendidas dentro do prazo regulatório.
- **Supervisão Permanente e Canais Críticos** | Em 2024, respondemos 56 ofícios da Supervisão Permanente e dos Canais, sendo todos atendidos dentro do prazo estabelecido.

Além disso, todas as demandas da Auditoria Externa e Auditoria Interna são acompanhadas para assegurar que sejam devidamente atendidas.

Essas práticas garantem que estejamos sempre em conformidade, protegendo assim os interesses de todos os stakeholders.



Programa de Cultura de Gestão Baseada em Riscos

GRI 2-16 | 2-25

O Programa tem como objetivo promover uma cultura de prevenção aos riscos, compartilhando conceitos e comportamentos que inspirem positivamente nossos colaboradores no gerenciamento dos riscos no dia a dia.

Este ano, lançamos uma página no SharePoint (nosso portal interno) para disseminação de conceitos e boas práticas entre os colaboradores por meio de textos informativos, vídeos e instrumentos normativos, como o Código de Ética.

Para reforçar o compromisso e ampliar o conhecimento dos colaboradores sobre o tema, assim como disseminar as ferramentas de monitoramento disponíveis, lançamos o **Guia de Compliance**, que aborda, entre outros, o Código de Ética e Conduta, Integridade

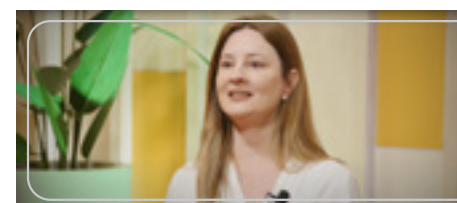
e Ética, e as Políticas e Procedimentos.

Também realizamos o 4º Workshop sobre a Cultura de Gestão Baseada em Riscos, com o tema “Segurança da Informação”, destinado aos colaboradores e membros dos órgãos estatutários. O evento contou com a participação de José Roberto Lama, da gerência de Governança de Segurança da Informação do Itaú Unibanco, como palestrante.

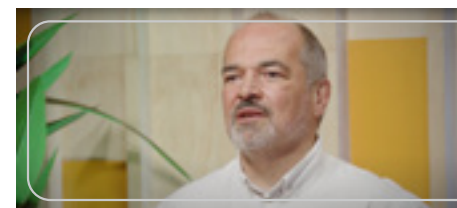
Continuidade de Negócios e Gestão de Crises

Nosso Programa de Continuidade de Negócios e Gestão de Crises tem como objetivo garantir que os processos essenciais continuem funcionando, minimizando os

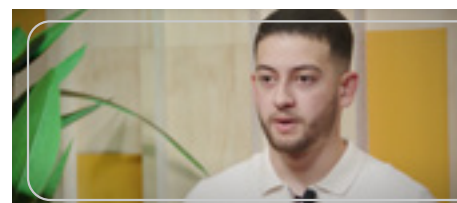
O Programa também incluiu a criação de uma série de vídeos para reforçar os riscos aos quais nossa organização está sujeita e que devem ser constantemente monitorados nas atividades diárias.



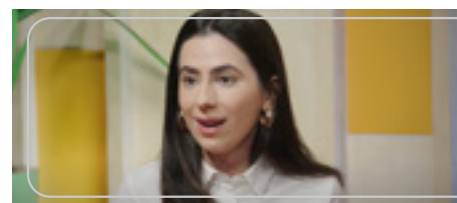
Gestão Baseada em Risco



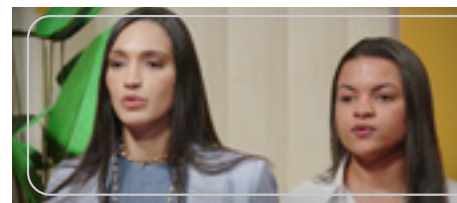
Riscos em Investimentos



Risco Atuarial



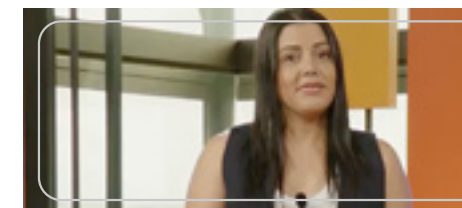
Riscos de SI e LGPD



Riscos Jurídicos, de Integridade e Ética e Compliance



Recursos Humanos



Seguridade



Comunicação



Controladoria



Governança

Em 2024, foram elaborados planos de contingência e realizados testes para oito processos classificados como críticos, obtendo resultados efetivos.



Auditoria Interna

A Auditoria Interna atua como terceira linha de defesa da Fundação. Sua atividade é independente e objetiva de avaliações de processos e riscos e de consultoria, desenhada para adicionar valor e melhorar as operações da organização, conforme definido na Estrutura Internacional de Práticas Profissionais (*International Professional Practices Framework* - IPPF) do The Institute of Internal Auditors - The IIA.

O resultado dos trabalhos da Auditoria Interna é registrado em relatório, contendo informações como: escopo, período avaliado, processos e riscos avaliados, opinião sobre o ambiente de controle, eventuais apontamentos de auditoria (situações expostas ao risco) e/ ou oportunidades de melhoria nos processos.

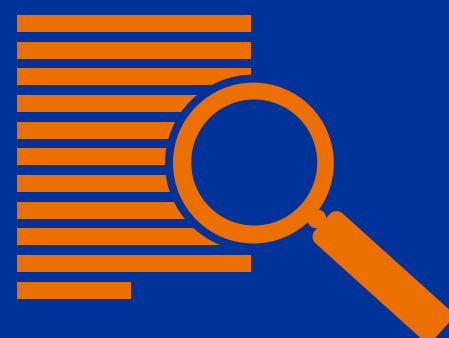
A metodologia adotada pela Auditoria Interna é orientada também pelo The IIA e está estruturada em 4 etapas:

- Planejamento anual;
- Execução dos trabalhos;
- Conclusão;
- *Follow-up*.



Em 2024, a Auditoria Interna cumpriu **100%** do planejamento previsto para o ano, que contemplou **5 trabalhos de auditoria.**

O resultado dos trabalhos foi apresentado para as alçadas devidas com emissão de relatórios. Apontamentos de auditoria são registrados em sistema dedicado para monitoramento dos planos de ação e prazos definidos em política interna.



Processo	Resultado
Processos Judiciais	Moderado +
Gestão de Cadastro	Moderado +
Gestão Atuarial	Moderado +
Gestão de Investimentos	Moderado +
Monitoramento Fornecedores (KYS)	Atende





www.fundacaoitauunibanco.com.br

