ABC BRASIL DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS S.A – "DTVM"

Procedimentos:	**Código.Versão:**
Metodologia de Gestão de Risco Operacional e Controle Internos	**3231.PRC.01**

Para qualquer dúvida relativa a esta política, falar com:

Gestão de Riscos

Risco Operacional

Esta política aplica-se à DTVM, seus funcionários, filiais e subsidiárias. Em caso de conflito entre esta política e as legislações locais onde se encontram as representações do exterior impossibilitando seguir as disposições aqui contidas, os pedidos de exceção deverão seguir as diretrizes determinadas em políticas específicas.

Gestor: Gestão de Risco Operacional

Aprovado por: Vice-Presidência

Usuários: Área de Gestão de Risco Operacional; Comitê Executivo; Comitê de Risco Operacional, Compliance e Segurança da Informação (CROCS); Agentes de Risco Operacional.

Índice

1. TERMOS E DEFINIÇÕES - 3 -
2. OBJETIVO - 6 -
3. DIRETRIZES DA METODOLOGIA DE GESTÃO DO RISCO OPERACIONAL - 7 -
4. PAPÉIS E RESPONSABILIDADES - 7 -
5. VISÃO GERAL - 10 -
6. CLASSIFICAÇÃO DE RISCO - 10 -
7. DICIONÁRIO DE RISCOS OPERACIONAIS (TAXONOMIA) - 13 -
8. PROCESSOS DA METODOLOGIA - 14 -
9. SISTEMAS E APLICATIVOS - 25 -
10. RISCO OPERACIONAL EM FORNECEDORES RELEVANTES - 28 -
11. RISCO OPERACIONAL EM NOVOS PRODUTOS, PROCESSOS E SISTEMAS - 29 -
12. CAPITAL REGULATÓRIO DE RISCO OPERACIONAL - 29 -
13. REGULAMENTAÇÕES E REFERÊNCIAS - 30 -

Histórico:

Versão	Data	Descrição	Gestor

01	30/08/2023	Criação Metodologia de Gestão de Risco	Riscos Operacionais e Controles Internos

Nota: Este manual deve ser revista pelo Gestor anualmente ou em menor período caso necessário.

1. Termos e Definições

Termo	Definição

Risco Operacional	Risco operacional é possibilidade da ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas. Esta definição inclui o risco legal associado à inadequação ou deficiência em contratos firmados pela instituição, às sanções em razão de descumprimento de dispositivos legais e às indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.
Incidente ou Evento de Risco Operacional	Evento ou incidente é um possível acontecimento que leva materialização do Risco Operacional, podendo resultar ou não em perdas operacionais. Para fins regulatórios e de categorização, a **DTVM** utiliza as mesmas definições adotadas pela Resolução 4.557/17 do Banco Central do Brasil e classifica os eventos de risco operacional em 8 (oito) categorias, a saber: 1. fraudes internas; 2. fraudes externas; 3. demandas trabalhistas e segurança deficiente do local de trabalho; 4. práticas inadequadas relativas a clientes, produtos e serviços; 5. danos a ativos físicos próprios ou em uso pela instituição; 6. situações que acarretem a interrupção das atividades da instituição; 7. falhas em sistemas, processos ou infraestrutura de tecnologia da informação (TI); 8. falhas na execução, no cumprimento de prazos ou no gerenciamento das atividades da instituição.
Evento de Crise	Crise é um incidente com impacto negativo classificado como "Muito Alto" de acordo com a Classificação de Impacto de Risco da **DTVM** , podendo resultar ou não em situações que levem à interrupção de negócios.
Evento de Risco Cibernético	Define-se como tentativas de comprometer a confidencialidade, integridade e disponibilidade de dados ou sistemas tecnológicos.
Causa de Risco Operacional	Motivos que levaram o evento de risco a ocorrer. Representa a origem do problema e explica a natureza do risco. Os eventos podem ter uma ou mais causas associadas. Para fins de categorização a **DTVM** utiliza as mesmas definições adotadas pelo Comitê de Basileia e classifica as causas em: 1. Pessoas; 2. Processos internos; 3. Eventos externos; 4. Sistemas e infrastrutura.

Risco Operacional Inerente	Representa o Risco Operacional sem um ambiente de controles internos (ou seja, fatores de mitigação ou tratamentos) aplicado.
Risco Operacional Residual	Representa o Risco Operacional que permanece após a aplicação de controles internos para sua mitigação.
Controles Internos	Procedimentos, atividades ou mecanismos desenvolvidos para assegurar que atividades e processos sejam executados dentro de determinado padrão, assegurando que os objetivos da **DTVM** sejam atingidos e que eventos de risco sejam prevenidos ou detectados e corrigidos.
Primeira Linha de Defesa (1ª LDD)	A 1ª LDD refere-se aos proprietários de negócios e processos cujas atividades criam e / ou gerenciam os riscos operacionais que podem facilitar ou impedir que os objetivos de uma organização sejam alcançados. Isso inclui inclusive assumir os riscos certos, em linha com o apetite de riscos da **DTVM**. A 1ª LDD é responsável pelo o risco, e pelo design e execução dos controles internos para responder a esses riscos. No contexto da **DTVM**, refere-se todas as áreas de negócio e de suporte à negócio.
Segunda Linha de Defesa (2ª LDD)	A 2ª LDD apoia e desafia a gestão de risco operacional executada pela 1ª LDD para de forma a garantir que os riscos e controles internos sejam gerenciados de forma eficaz, através do desafio do resultado do monitoramento executado pela 1ª LDD de seus riscos e da qualidade do seu ambiente de controles. As funções da 2ª LDD são separadas do 1ª LDD, mas ambas estão sob a direção da alta administração. A 2ª LDD é uma função de supervisão, responsável pela definição da metodologia de gestão de riscos e pelas atividades de disseminação da cultura de gestão de riscos. No contexto da **DTVM**, a 2ª LDD inclui as áreas de Gestão de Riscos Operacionais & Controles Internos e Compliance.
Terceira Linha de Defesa (3ª LDD)	A 3ª LDD fornece a indicação para a alta administração e para o Conselho de que os esforços da 1ª LDD e 2ª LDD na gestão dos riscos operacionais estão consistentes com as expectativas da diretoria e da alta gestão. A 3ª LDD normalmente não executa funções de gerenciamento para proteger sua objetividade e independência organizacional. Além disso, a 3ª LDD tem uma linha de reporte direta para o Conselho. Portanto, a 3ª LDD possui uma função garantidora e não uma função de gestão, que a separa da 2ª LDD. No contexto da **DTVM**, refere-se à Auditoria Interna.

Agente de Risco Operacional	Os agentes de Risco Operacional são colaboradores que pertencem à 1ª LDD e que auxiliam na identificação, avaliação, monitoramento e reporte dos eventos de risco operacional em atividades, processos e sistemas dentro da esfera de atuação das áreas em que estão alocados. Também atuam como disseminadores da cultura de gestão de risco.
Plano de Ação	Solução apresentada / gerenciada pela 1ª LDD e aprovada / monitorada pela 2ª LDD para resolver um ponto de risco operacional.
Perda Operacional	Representa impacto negativo e quantificável na Demonstração de Resultados da **DTVM** devido a um incidente de Risco Operacional e também despesas operacionais relacionados a questões trabalhistas, cíveis e fiscais. (classificadas como provável).
Nearmiss	Representa o conceito de "quase perda", ou seja, o funcionamento de um controle que impede a materialização da perda. Demais eventos fortuitos (devido ao acaso) também podem resultar em *nearmiss*.
Recuperação	Representa a materialização positiva e quantificável na Demonstração de Resultado da **DTVM** de uma perda operacional recuperada parcial ou totalmente.
Ganho	Representa impacto positivo e quantificável na Demonstração de Resultados da **DTVM** devido a um incidente de Risco Operacional.

2. Objetivo

A gestão de risco operacional tem como objetivos identificar, mensurar e avaliar, dar resposta aos riscos operacionais da organização, monitorá-los com a finalidade de manter as perdas e os riscos dentro dos limites estabelecidos pela **DTVM**.

Os gestores das diversas áreas da **DTVM** gerenciam os seus riscos e para tal se utilizam de metodologia, ferramentas e políticas corporativas construídas e disponibilizadas pela Área Gestão de Risco Operacional.

Este manual visa definir e descrever a metodologia e as ferramentas de gestão de risco operacional e controles internos e como elas se articulam entre si. Com isto,

objetiva-se a padronização de procedimentos e avaliações que são, muitas vezes, de natureza subjetiva.

3. Diretrizes da Metodologia de Gestão do Risco Operacional

A metodologia de gestão de risco operacional deve ser consistente em sua abordagem e incluir:

- Aderência ao modelo das Três Linhas de Defesa;
- Melhoria contínua da estrutura de gestão de riscos operacionais existente;
- Taxonomia de risco comum;
- Metodologia de classificação de risco uniforme;
- Processos de gestão de risco operacional que consistem em:
  - ✓ Coleta de dados de perda operacional e gerenciamento de incidentes;
  - ✓ Autoavaliações de riscos e controles, incluindo o estabelecimento de indicadores-chave de risco,
  - ✓ Gestão de pontos de risco operacional e planos de ação relacionados;
  - ✓ Testes e revisões de controles internos.

- Sistemas e aplicativos relacionados.

As iniciativas de gestão de risco operacional se concentram principalmente em avaliações baseadas nos principais riscos e em assuntos materiais e relevantes para a **DTVM** .

4. Papéis e Responsabilidades

A governança de gestão risco operacional da **DTVM** está alinhada às recomendações sugeridas pelo Comitê de Basileia e às determinações dos órgãos reguladores nacionais e internacionais, compreendendo pessoas, processos, ferramentas, sistemas e canais de informação que funcionam de forma coordenada.

Essa governança está baseada no conceito das Três Linhas de Defesa, cada uma com seus papéis e responsabilidades.

1º Linha de Defesa (1ª LDD)

Responsável primária por identificar, avaliar, testar, tratar, controlar, monitorar e reportar os riscos e controles de suas áreas, de forma alinhada às diretrizes internas, regulamentações, políticas e procedimentos aplicáveis.

Isso significa que a 1ª LDD deve:

- A 1ª LDD é responsável pela gestão de riscos operacionais, incluindo:
  - ✓ Identificar, avaliar, mensurar e reportar riscos
  - ✓ Reportar incidentes de risco operacional e eventos de perda operacional de forma tempestiva;
  - ✓ Realizar autoavaliação de controles para identificar se performam adequadamente;
  - ✓ Elaborar e atualizar a matriz de risco e controle
  - ✓ Definir e implementar planos de ação para a mitigação de riscos operacionais;
  - ✓ Disponibilizar recursos suficientes para a gestão de riscos operacionais;
  - ✓ Garantir o treinamento adequado e melhorar a consciência de risco da equipe;
  - ✓ Realizar análise de riscos operacionais e controles associados a novos produtos e projetos antes do seu lançamento;
  - ✓ Reportar indicadores chave de risco;
  - ✓ De forma proativa, identificar fragilidades no ambiente de controle e outras vulnerabilidades em seus processos e atividades através de auto apontamentos de risco operacional.

- Os gestores das linhas de negócios / suporte são assistidos por um ou mais Agentes de Risco Operacional, indicados pela própria 1ª LDD.

2º Linha de Defesa (2ª LDD)

Proprietária e custodiante das metodologias e ferramentas de gestão dos riscos operacionais da **DTVM** .

A 2ª LDD é responsável por:

- Garantir que as políticas, padrões e procedimentos relacionados à risco operacional estão atualizados e adequados para a sua finalidade;
- Fornecer treinamento para garantir que as políticas, padrões e procedimentos relacionados à risco operacional sejam compreendidos;
- Auxiliar a 1ª LDD na implementação do arcabouço de gestão de risco operacional;
- Monitorar a implementação de vários componentes aprovados do arcabouço de gestão de riscos operacionais e os Planos de Ação relacionados;
- Desafiar a análise de incidentes, pontos de risco operacional e indicadores-chave de risco, realizando seu reporte para a alta administração e demais partes interessadas;
- Coordenar e facilitar a execução de auto avaliações de risco e o reporte de incidentes e indicadores-chave de risco;
- Reportar os dados de gestão de risco operacional (financeiros e não financeiros) para as partes interessadas internas e externas.
- Ponto de contato para as partes interessadas, reguladores e auditores internos e externos para assuntos relacionados à gestão de riscos operacionais;
- Coordenar e facilitar a implementação local ou a solicitação de dispensa (conforme processo estabelecido) dos padrões e controles de riscos operacionais definidos pelo Grupo ABC;
- Fomentar cultura de consciência de risco.

3º Linha de Defesa (3ª LDD)

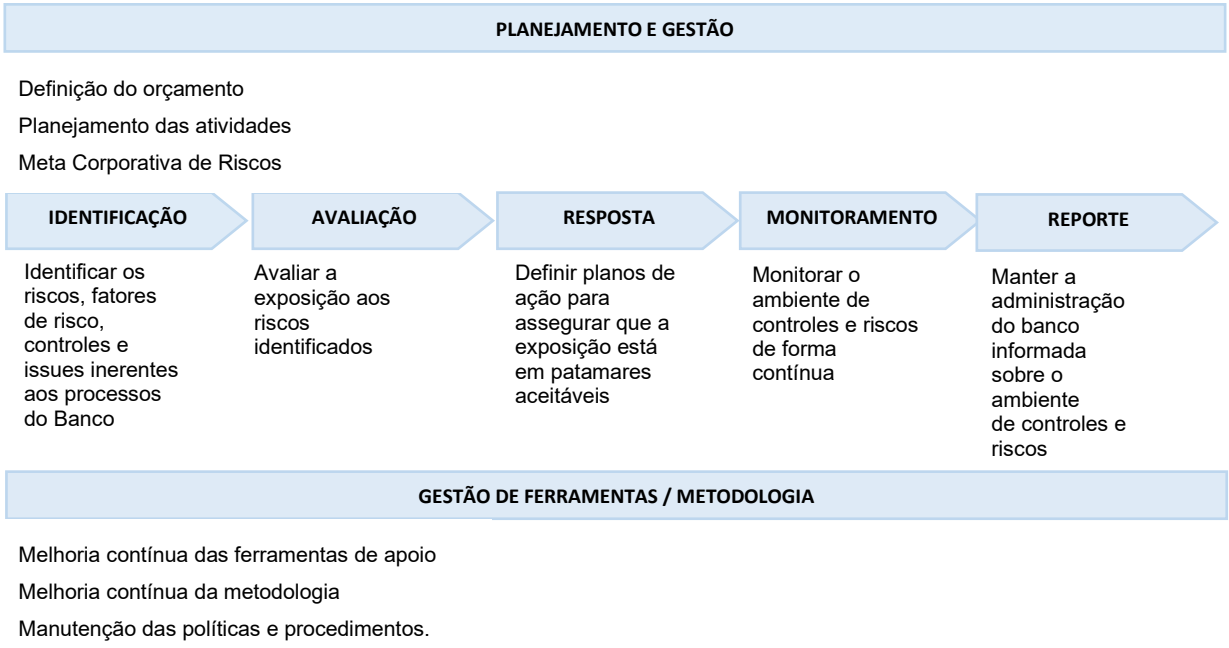
A Auditoria Interna é responsável pela asseguração independente e razoável quanto à efetividade do sistema de controles internos, gerenciamento de riscos, governança corporativa e gerenciamento de capital (incluindo aderência as leis e aspectos regulatórios).

A autoridade e mandato da Auditoria Interna é aprovado pelo Conselho de Administração e Comitê de Auditoria e, para cumprir com o mandato, a Auditoria Interna tem acesso irrestrito às operações, colaboradores e propriedades da **DTVM**.

5. Visão Geral

O *framework* da Metodologia de Gestão de Risco Operacional (doravante Metodologia) pode ser definido conforme abaixo:

FIGURA 1: METODOLOGIA DE GESTÃO DE RISCO OPERACIONAL – VISÃO GERAL



A Metodologia está alinhada ao COSO-ERM (Committee of Sponsoring Organizations of the Treadway Commission), no que se refere a controle interno.

6. Classificação de Risco

O objetivo da Classificação de Risco é obter melhor compreensão dos riscos através da determinação do impacto esperado e a probabilidade de ocorrência do evento de risco.

A Classificação de Risco define uma escala para avaliação:

- do impacto de um risco; e
- da probabilidade de um risco se materializar.

Impacto

As escalas de impacto devem ser usadas para a avaliação e classificação de "inerente" e "residual" dos riscos avaliados.

O risco inerente é o risco existente na ausência de qualquer ação que a gestão possa fazer para alterar a probabilidade ou impacto do risco.

Já o risco residual é o risco que permanece após a implementação das medidas definidas pela gestão para o tratamento do risco.

O impacto de um risco deve sempre ser avaliado para cada uma das seguintes dimensões:

- **Financeiro:** Régua única para todos os departamentos da **DTVM** , em BRL;
- **Reputacional:** o ativo mais importante de uma instituição financeira é a sua reputação. Questões de reputação podem resultar em perdas financeiras significativas, caso não forem corretamente e proativamente gerenciadas;
- **Clientes e funcionários:** a interrupção de serviços ou indisponibilidade de sistemas - oferecidos pela **DTVM** ou por terceiros - pode afetar negativamente nossos clientes e funcionários (operações) e levar a um impacto direto financeiro, de reputação ou regulatório quando não for adequadamente gerenciado;
- **Regulamentação e Compliance:** são particularmente importantes as relações da **DTVM** com seus reguladores locais e da matriz, uma vez que eles são responsáveis pelas licenças e autorizações para operar e expandir nossos negócios.

Um único incidente pode ter múltiplos impactos, cada um eventualmente demandando avaliação separada.

Os eventos de riscos relacionados aos incidentes e problemas devem sempre ser avaliados da perspectiva da **DTVM** .

A classificação do impacto de um evento não é uma ciência exata. O evento deve ser classificado sempre de acordo com sua "pior" pontuação para qualquer uma das 4 dimensões, conforme tabela abaixo:

TABELA 1: CLASSIFICAÇÃO DE RISCO UNIFORME – RÉGUA DE IMPACTO DE RISCO

NÍVEL DE IMPACTO	TIPO DE IMPACTO (MAIS RELEVANTE)			
	FINANCEIRO (Em Reais)	REPUTACIONAL (mídias tradicional e social)	CLIENTES E FUNCIONÁRIOS	REGULATÓRIO E COMPLIANCE
Muito Alto	Acima de 5 milhões	Atenção negativa da mídia internacional a longo prazo	Acima de 40% dos clientes impactados E/OU Acima de 40% dos funcionários impactados	- Multa ou penalidade regulatória de R$ 500 mil ou acima e / ou; - Revogação da licença / restrições à licença concedida e/ou; - Evento a ser relatado ao regulador diretamente ou como parte do ciclo de relatório regular com provável nível de interesse muito alto pelo regulador.
Alto	Entre 1 milhão e 5 milhões	Atenção negativa da mídia nacional a longo prazo	Entre 15% e 40% dos clientes impactados E/OU Entre 15% e 40% dos funcionários impactados	- Multa ou penalidade regulatória entre R$ 50 mil e R$ 500 mil e / ou; - Aviso formal do regulador para evento material que se repetido no futuro pode levar a consequências com impacto Muito Alto e/ou; - Evento a ser relatado ao regulador diretamente ou como parte do ciclo de relatório regular com provável nível de interesse alto pelo regulador.
Médio	Entre 250 mil e 1 milhão	Atenção negativa da mídia local a curto prazo	Entre 5% e 15% dos clientes impactados E/OU Entre 5% e 15% dos funcionários impactados	- Multa ou penalidade regulatória regulatória entre R$ 5 mil e R$ 50 mil e / ou; - Aviso formal ou comentários negativos do regulador (mesmo verbais) para eventos não-materiais e/ou; - Evento a ser relatado ao regulador diretamente ou como parte do ciclo de relatório regular com provável nível de interesse médio pelo regulador.
Baixo	Abaixo de 250 mil	Atenção negativa limitada da mídia local / sem atenção da mídia	Abaixo de 5% dos clientes impactados E/OU < 5% dos funcionários impactados	- Multa ou penalidade regulatória inferior a R$ 5 mil e / ou; - Evento a ser relatado ao regulador diretamente ou como parte do ciclo de relatório regular com provável nível de interesse baixo pelo regulador.

Probabilidade

Define-se como probabilidade a indicação da chance de ocorrência de um incidente tendo como referência o período pré-determinado.

Somente eventos de risco plausíveis devem ser abordados. Para efeitos dessa Metodologia, eventos plausíveis são eventos que, de acordo com uma opinião qualificada, podem ocorrer em um futuro previsível ou para os quais não existem argumentos sólidos para declarar com segurança que eles não vão / não podem acontecer.

A **DTVM** usa uma escala de 4 níveis para classificar a probabilidade de ocorrência (freqüência) dos eventos de risco identificados, conforme tabela abaixo:

TABELA 2: CLASSIFICAÇÃO DE RISCO UNIFORME – RÉGUA DE PROBABILIDADE DE RISCO

NÍVEL DE FREQUENCIA	DEFINIÇÃO
Muito Provável	O evento identificado é muito provável que (re) ocorra, possivelmente com freqüência. Ocorrem regularmente em bancos; são relatados na imprensa a cada 3 a 6 meses; existem vários registros no banco de dados de incidentes do Banco.
Provável	O evento identificado é provável que aconteça, mas não é um problema ou circunstância persistente. Ocorrem regularmente em bancos; são relatados a cada 6 a 24 meses na imprensa; alguns eventos podem ter sido registrados no banco de dados de incidentes do Banco.
Possível	O evento identificado pode acontecer. São eventos de risco que podem ocorrer caso sejam criadas certas condições propícias para a sua materialização. São relatados a cada 2 a 5 anos na imprensa.
Remoto	O evento identificado é provável que nunca aconteça ou se materialize, embora não possa ser excluído. São eventos de risco plausíveis, mas muito raros e difíceis de prever e que estão além do âmbito das expectativas normais na história, ciência, finanças ou tecnologia. São relatados a cada 5 anos ou mais na imprensa. Podem ou não ter se materializado no passado. Não podem ser cientificamente considerados, com um alto grau de certeza, de que nunca se materializarão.

Matriz de Classificação de Risco

A **DTVM** classifica seus riscos operacionais, usando a Matriz de Classificação de Risco. Todos os riscos operacionais são classificados como "Crítico", "Significativo", "Moderado" ou "Mínimo" com base em seu impacto e probabilidade, conforme abaixo:

TABELA 3: CLASSIFICAÇÃO DE RISCO– MATRIZ DE CLASSIFICAÇÃO

	CLASSIFICAÇÃO DE RISCO				
IMPACTO	MUITO ALTO	MODERADO	SIGNIFICANTE	CRÍTICO	CRÍTICO
	ALTO	MODERADO	SIGNIFICANTE	SIGNIFICANTE	CRÍTICO
	MÉDIO	MÍNIMO	MODERADO	MODERADO	SIGNIFICANTE
	BAIXO	MÍNIMO	MÍNIMO	MÍNIMO	MODERADO
		REMOTO	POSSÍVEL	PROVÁVEL	MUITO PROVÁVEL
		PROBABILIDADE			

7. Dicionário de Riscos Operacionais (Taxonomia)

O Dicionário de Riscos Operacionais é uma taxonomia definida pela área de Gestão de Risco Operacional e Controle Interno para a **DTVM** , baseada nos conceitos apresentados pelo Comitê de Basiléia de Compensações Internacionais (Bank of

International Settlements – BIS), pelo Sistema de Auto Regulação Bancária da Federação Nacional dos Bancos do Brasil (SARB – FEBRABAN) e outras boas práticas recomendadas para a gestão de riscos operacionais

A taxonomia de risco é um elemento muito importante da estratégia de gestão de risco operacional e define uma nomenclatura comum de categorias de risco que deve ser usada por todo a **DTVM** com o objetivo de garantir a consistência e uniformidade na identificação, avaliação da sua exposição e definição dos objetivos de gerenciamento desses riscos.

A taxonomia de risco fornece a base para uma abordagem mais estruturada e holística para o gerenciamento de risco, permitindo:

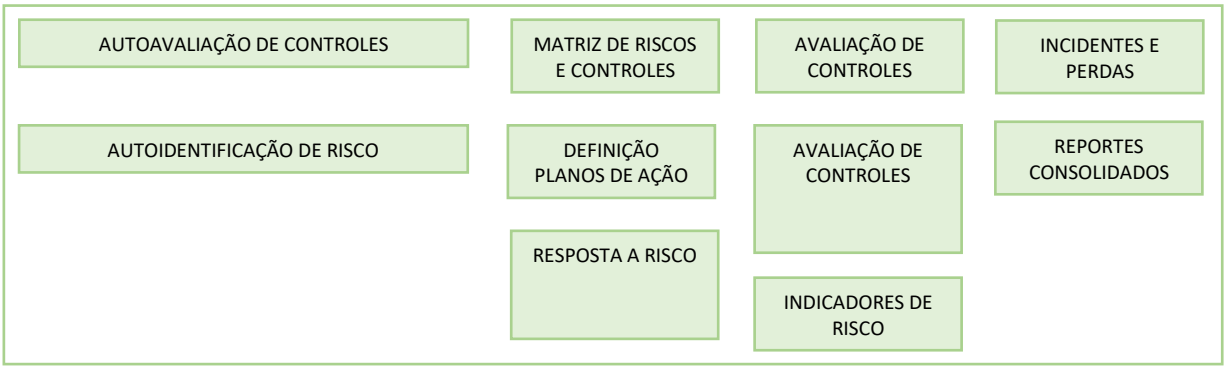
- Identificar os vetores dos principais riscos que afetam a **DTVM** ;
- Definir as abordagens para mensuração dos riscos;
- Definir o apetite de risco para os vários riscos;
- Definir uma governança adequada para a gestão dos diversos riscos;
- Classificar / mapear dados de risco (incluindo incidentes, indicadores, controles, etc.).

O Dicionário de Riscos Operacionais é mutuamente exclusivo (ou seja, os riscos não se sobrepõem) e coletivamente exaustiva (ou seja, não há lacunas). Ao selecionar a categoria de risco apropriada, deve-se sempre preferir a mais específica em vez da mais genérica.

8. Processos da Metodologia

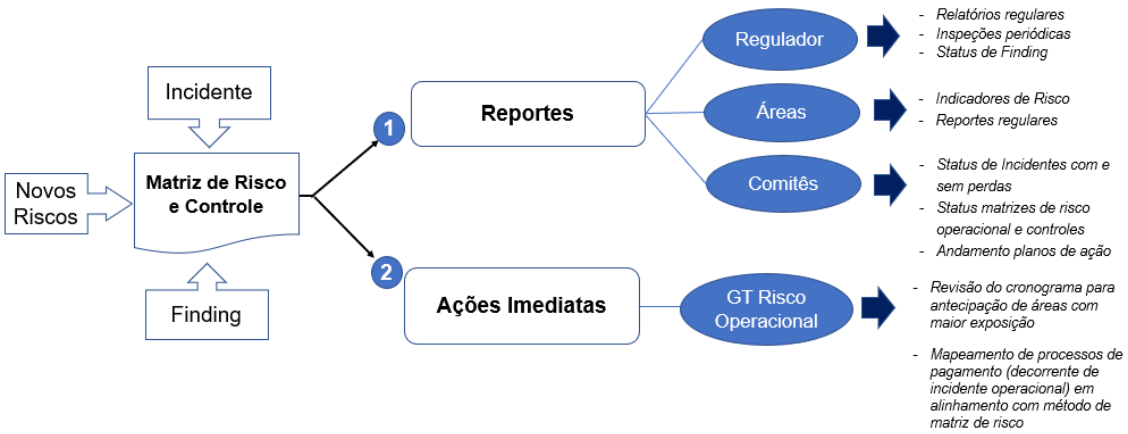
Para o desenvolvimento e implementação do arcabouço de gestão de risco operacional na **DTVM** em linha com a metodologia definida, a área de Gestão de Risco Operacional e Controle Interno faz uso de uma série de processos conforme demonstrado a seguir:

FIGURA 3: METODOLOGIA DE GESTÃO DE RISCO OPERACIONAL – PROCESSOS



8.1. Matriz de Riscos e Controles

A Matriz de Riscos e Controles (MRC) representa a avaliação de seus riscos inerente e residual da área e seus respectivos controles associados que mitigam eventual materialização. A 2ª Linha de Defesa (LDD) nesse processo tem a função de desafiar e trazer aspectos eventualmente desconsiderados nessa avaliação pela 1ª LDD. A matriz é dinâmica e deve sempre ser atualizada pela 1ª LDD quando da ocorrência de incidentes, finding de auditoria e/ou surgimento de novos riscos que levam a uma atualização/reavaliação.



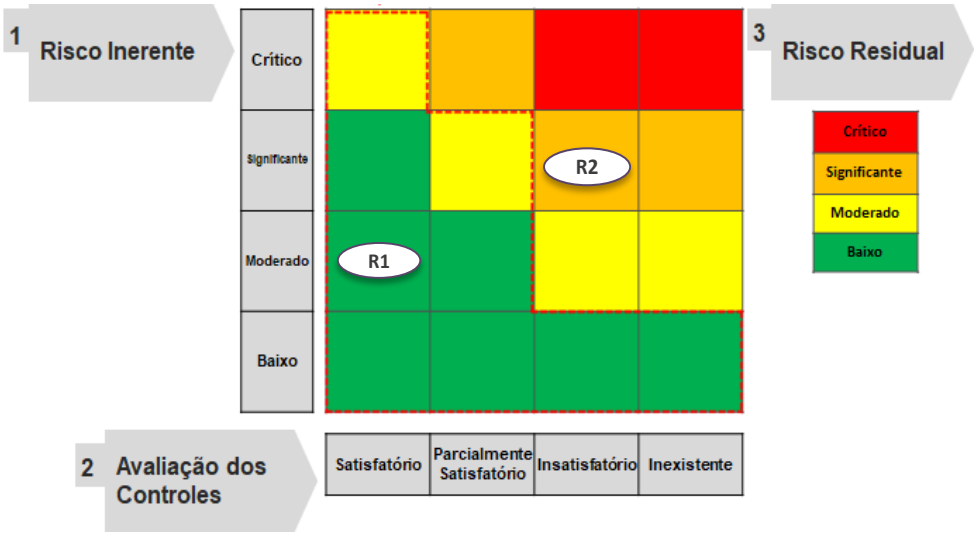
Mapa de Riscos Priorizados (*heat map*)

O Mapa de Riscos Priorizados (MRP ou *Heat Map*) corresponde à representação gráfica dos principais eventos de risco mapeados na MRC.

Informação para uso interno

Riscos residuais avaliados como crítico e significante devem ser levados ao conhecimento do CROCS com respectivas ações mitigatórias e acompanhadas para que se evidencie se as eventuais ações tomadas e/ou em curso produzam efeitos que reduzam sua severidade residual.

FIGURA 5: MAPA DE RISCOS PRIORIZADOS (HEAT MAP)



8.2. Autoavaliação de Controles (CSA – *control self assessment*)

O processo de autoavaliação de controle deve garantir que a 1ª LDD analise, reflita e avalie controle vis a vis a exposição do risco sob sua responsabilidade. Para realização desta avaliação a 1ª LDD, deve considerar, mas não se limitar aos instrumentos de risco operacional, como controles internos, indicadores chave de risco, pontos de risco operacional e planos de ação para definir o risco residual.

FIGURA 4: AUTOAVALIAÇÃO DE CONTROLES

Deve ser apresentado no Comitê de Riscos Operacionais, Compliance e Segurança da Informação (CROCS) o resultado e Cronograma Anual de Auto Avaliações de Controles.

8.3. Auto Identificação de Risco/*Issues* (*self Identified issue*)

A auto identificação de issues é um processo que permite que riscos e pontos fracos de controle sejam identificados preventivamente pela 1ª LDD (ou seja, antes de o problema ser levantado pela segunda ou terceira linha de defesa, ou mapeado durante o cronograma de autoavaliação, por exemplo), independentemente de como a deficiência de controle foi identificada.

Uma vez auto identificado pela 1ª LDD, o risco deve ser reportado para a área de Gestão de Risco Operacional e Controle Interno através de formulário específico (ver *Anexo 2*) e a resposta ao risco, uma vez definida, será monitorada.

8.4. Planos de Ação e Assunção de Risco

Como parte do processo de reposta aos riscos operacionais, todo o risco deve ser:

- **Mitigado:** Medidas tomadas para reduzir o impacto e / ou probabilidade do evento de risco; ou

Informação para uso interno

- **Transferido:** por exemplo segurado, garantido por terceiro, etc .; ou
- **Aceito:** o impacto e a probabilidade do evento de risco são aceitos.

É requerido obter aprovação de *risk acceptance* (seguindo formulário existente para essa finalidade) através do CROCS caso se tenha risco residual avaliado ou reavaliado para significante/crítico, sem controle apropriado e após a implementação de ações mitigatórias de controle.
Caso o risco tenha relação com questões regulatórias, Compliance deve ser consultado. Vale mencionar que se a área possui risco residual avaliado como moderado ou acima deve ser apresentado ao CROCS para ciência.

- **Encerrado:** as atividades que originam o risco são encerradas.

As decisões reais sobre o tratamento de um risco devem ser baseadas na análise das causas subjacentes e os controles já instalados. A decisão também deve levar em consideração a probabilidade e o impacto, o contexto mais amplo, como a disponibilidade de recursos para corrigir problemas, o tempo para corrigi-los, introdução planejada de novos sistemas, reorganizações, etc.

Planos de Ação

Caso a resposta ao risco definida envolva o desenvolvimento de um plano de ação, ele deve contemplar no mínimo as seguintes etapas:

- Mapeamento / diagnóstico detalhado da causa-raiz;
- Identificação dos gaps de controles;
- Definição das ações necessárias para a mitigação do evento risco.

Os planos de ação são definidos pelas áreas envolvidas, a qual é responsável pelo acompanhamento do plano. O Cadastro do plano é de responsabilidade do owner que pode estar na 1ª ou 2ª LDD.

Riscos classificados como "Crítico" ou "Significativo" ou incidentes com impacto efetivo definido como "Alto" ou "Muito Alto" cuja açâo mitigatória tenha prazo de implementação acima de 30 dias devem obrigatoriamente ter um Plano de Ação correspondente registrados no aplicativo Controle Corporativo de Planos de Ação para acompanhamento da área de Riscos Operacionais e Controles Internos, conforme item *9.2. Controle Corporativo de Planos de Ação* desse manual.

Um plano de ação só será registrado após o alinhamento prévio e autorização do gestor da área responsável pela condução do plano (owner). Porém, caso um plano já registrado seja posteriormente rejeitado pelo gestor da área responsável,

independentemente do motivo, o mesmo será levado à ciência do CROCS para possível tomada de decisão. Reprogramações devem ser levadas ao CROCS para ciencia..

Os planos derivados de exigências regulatórias são do escopo de atuação da área de Compliance.

Planos de ação relacionados à incidentes que envolvem risco cibernético ou que forma definidos como 'crises' devem estar alinhados com as diretrizes definidas nos documentos internos *3740.ORG - Plano de Resposta a Incidentes* e *4060.ORG - Gestão de Crises* , respectivamente.

Os planos de ação devem ser encerrados pelos respectivos gestores responsáveis.

Planos de ação encerrados sem a devida comprovação de sua conclusão poderão ser reabertos pela Área de Gestão de Risco Operacional e Controles Internos.

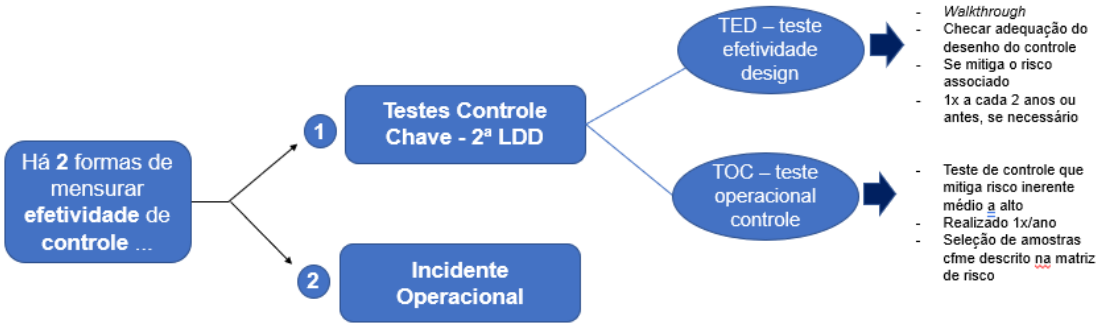
8.5. Testes de Controle de 2ª LDD

A **DTVM** possui estrutura de controle formada pelas 3 linhas de defesa que proporciona à alta administração segurança de que o ambiente de controles internos esteja funcionando corretamente.

A 1ª LDD deve realizar monitoramento contínuo de seus respectivos controles chave.

A 2ª LDD estabelece e mantém o arcabouço de gestão de risco operacional e controles através dos testes de design e operacional dos controles-chave da **DTVM** que mitiguem riscos inerentes avaliados como crítico e/ou significante.

A 3ª LDD audita o arcabouço e a pertinente implantação dos conceitos preconizados nessa metodologia.



8.6. Indicadores Chave de Risco

Os indicadores-chave de risco representam medida que fornece informação sobre o nível de exposição da **DTVM** a um dado evento de risco operacional num determinado ponto no tempo.

Idealmente, os indicadores são números relativos, devendo ser comparados com valores limiares que indicam se os processos avaliados se apresentam em situação normal, de alerta ou de atenção. Se um indicador começa a se aproximar do limite de capacidade de processamento de uma área, por exemplo, pode-se de antemão tomar uma providência, como investimento em TI, contração de pessoal, horas extras, etc.

A 1ª LDD é responsável pela decisão de quais indicadores serão monitorados, sua geração e a qualidade da informação fornecida.

Em suma, por meio dos indicadores de riscos, é possível:

- relacionar os eventos com suas causas, suas conseqüências, ou seus sintomas;
- comprovar os efeitos das medidas de mitigação de riscos;
- apoiar decisões sobre aumentar, reduzir ou transferir o risco;
- avaliar a alteração dos níveis de alerta e atenção em função de melhora dos controles, ou de mudanças de conjuntura;
- antecipar probabilidade de incidentes.

Principais questões a se levar em conta na criação e seleção de indicadores-chave de risco:

- os indicadores precisam ser relevantes, devendo ser relacionados à eventos de risco que precisem de monitoramento constante;
- os indicadores devem ser de fácil compreensão e interpretação;
- os indicadores devem ser auditáveis;
- os indicadores devem ter responsável por eles;
- os indicadores devem variar diretamente em função do risco ou da qualidade dos controles monitorados.

Por outro lado, uma melhora em indicadores podem indicar o efeito de ações de redução do risco decorrentes de ações tomadas para o aprimoramento de controles.

É importante que se mantenha o histórico de evolução dos indicadores, já que eles estão relacionados a conjuntura de eventos externos, mercado ou das atividades da **DTVM** e fazem sentido devidamente contextualizados.

8.7. Incidentes e Perdas Operacionais

O processo de gestão de incidentes da **DTVM** define os princípios básicos e práticas para a identificação, reporte e registro de incidentes de risco operacional e eventos de perda operacional.

Os princípios e práticas do processo de gestão de incidentes e perdas operacionais se alinham com as demandas regulatórias atuais e com as melhores práticas da indústria.

Reporte e Registro de Incidentes

Os incidentes são uma importante fonte de indicação de falhas de processo ou de controles e devem ser analisados afim de se verificar a necessidade de revisão das informações mapeadas durante o processo de autoavaliação de riscos e controles e a criação de planos de ação para a mitigação dos eventos de risco associados.

Além disso, uma base histórica bem estruturada de incidentes permite análise de lições aprendidas (*lessons learned*), funcionando como referência de resposta à riscos com base em incidentes semelhantes que já ocorreram.

É de responsabilidade da 1ª LDD a comunicação tempestiva sobre a ocorrência de incidentes de risco operacional na **DTVM** . A comunicação de um incidente é feita através de ferramenta de formulário específico disponível na Intranet da **DTVM**. Para mais detalhes, favor consultar item 9*.1 – Fluxo BPM de Reporte de Perdas e Incidentes* desse documento.

Estornos de valores à clientes cuja origem é um evento de risco operacional também são classificados como incidentes, porém sua comunicação / registro é feita através de ferramenta específica sob a gestão da área de Client Service. Para maiores detalhes, favor consultar o procedimento interno *6012.PRC – Manual do Client Service*.

No momento do registro de um pedido de requisição estorno, a área demandante indica a área de Riscos Operacionais e Controles Internos como uma das alçadas de aprovação caso se tratar de um estorno cuja origem é um evento de risco operacional.

Caso a área de Gestão de Risco Operacional conclua que o estorno enviado para análise não se enquadra como uma falha operacional, o estorno é classificado como 'acordo comercial' e não é registrado como incidente.

Perdas Operacionais

Representa impacto negativo e quantificável na Demonstração de Resultados da **DTVM** devido a um incidente de Risco Operacional. Consideramos para essa finalidade as despesas operacionais, incluindo provisões para questões trabalhistas, cíveis e fiscais (classificadas como provável).

As perdas operacionais são apuradas mensalmente pela Área de Gestão de Risco Operacional e Controle Interno e validadas de acordo com os lançamentos gerados pela Controladoria.

Perdas Operacionais Trabalhistas

Perdas Trabalhistas são perdas cujo evento de origem é a instalação de um processo trabalhista ou ação indenizatória movido por um ex-funcionário (contratado, temporário ou terceiro) contra a **DTVM** . Consideramos somente as ações classificadas como prováveis para efeito de cômputo na base de dados de perdas operacionais.

O processo de captura de perdas trabalhistas exige não só a análise das contas contábeis, mas também a identificação dos lançamentos por ação trabalhista correspondentes a cada valor, uma vez que cada ação equivale a um evento de perda.

Para auxiliar na identificação individual das ações trabalhistas e correto registro das perdas associadas, a equipe do Departamento Jurídico envia mensalmente as seguintes informações:

- Planilha de provisão trabalhista;
- Planilha contendo as perdas efetivas GFIP/Depósitos judiciais.

São consideradas perdas operacionais trabalhistas:

- Adições / reversões de provisão;
- Despesas com prestação de serviços de honorários trabalhistas;
- Custas judiciais (GRU/GFIP e depósitos judiciais).

Perdas Operacionais Cíveis

Perdas Cíveis são perdas cujo evento de origem é a instalação de um processo cível (ação) movido por uma Pessoa Física ou Jurídica contra a **DTVM**. Consideramos somente as ações classificadas como prováveis para efeito de cômputo na base de dados de perdas operacionais.

A identificação desse tipo de perda envolve a análise dos lançamentos registrados pela Controladoria no balancete mensal da **DTVM**.

O processo de captura de perdas cíveis exige não só a análise das contas contábeis, mas também a identificação dos lançamentos por ação cível correspondente a cada valor, uma vez que cada ação equivale a um evento de perda.

Perda Operacional Fiscal

Perdas Fiscais estão relacionadas geralmente a questões tributárias na esfera federal, estadual ou municipal onde a **DTVM** é polo passivo da ação classificada internamente como provável. Para efeito de base não consideramos obrigações

legais. O foco é exclusivamente casos onde ocorreram falha de interpretação da legislação vigente, perda de prazo, autuações de órgãos de governo.

A identificação desse tipo de perda envolve:

a) análise dos incidentes reportados para identificação daqueles com perda operacional associada.

b) análise dos lançamentos registrados pela Controladoria no balancete mensal da **DTVM** , nas contas contábeis

c) Planilha de provisão das ações fiscais;

Demais Perdas Operacionais

Certamente outras perdas estão no escopo de captura recorrente, pois a fonte de originação é variada e os incidentes com perda representam essa diversidade. Portanto, perdas que ocorrem no âmbito de tesouraria/mesa de operações, fraude em crédito, pagamentos em atraso para fornecedores dentre outras situações são registradas em outras contas contábeis distintas e que são consideradas em nossos registros e conciliação.

A identificação dessa natureza de perda envolve:

a) análise dos incidentes reportados para identificação daqueles com perda operacional associada.

d) a análise dos lançamentos registrados pela Controladoria no balancete mensal da **DTVM**, nas respectivas contas contábeis:

- **Serviços Processamento – CETIP;**
- **Multa de trânsito;**
- **Desp. Multas aplic. p/Banco Central;**
- **Multa dedutível;**
- **Multas;**
- **Multa indedutivel;**
- **Prejuízos operacionais;**
- **Juros.**

Ressalta-se que essas rubricas não são exaustivas, pois há outros incidentes que são registrados em contas contábeis regulares e que também podem entrar em nosso escopo dependendo do caso/situação que ocorreu.

8.8. Reportes

Os reportes contribuem para garantir que os principais elementos do arcabouço de gestão de risco operacional sejam comunicados a todas as áreas da **DTVM** de forma a apoiar e incentivar *accountability* e o senso de propriedade dos seus riscos operacionais.

Os principais reportes sobre gestão da área de Risco Operacional e Controles Internos estão relacionados ao CROCS, BRC, e reportes enviados as Áreas (conforme demanda).

9. Sistemas e Aplicativos

9.1. Fluxo BPM de Reporte de Incidentes

A comunicação de um incidente deve ser através de aplicativo de fluxo BPM, sob a gestão da área de Riscos Operacionais e cujo acesso está disponível na Intranet da **DTVM** , conforme abaixo:

FIGURA 6: APLICATIVO BPM DE REPORTE DE INCIDENTES E PERDAS OPERACIONAIS

O aplicativo de fluxo BPM também funciona como base histórica de incidentes, os quais podem ser extraídos através de reportes em formato MS Excel (planilha).

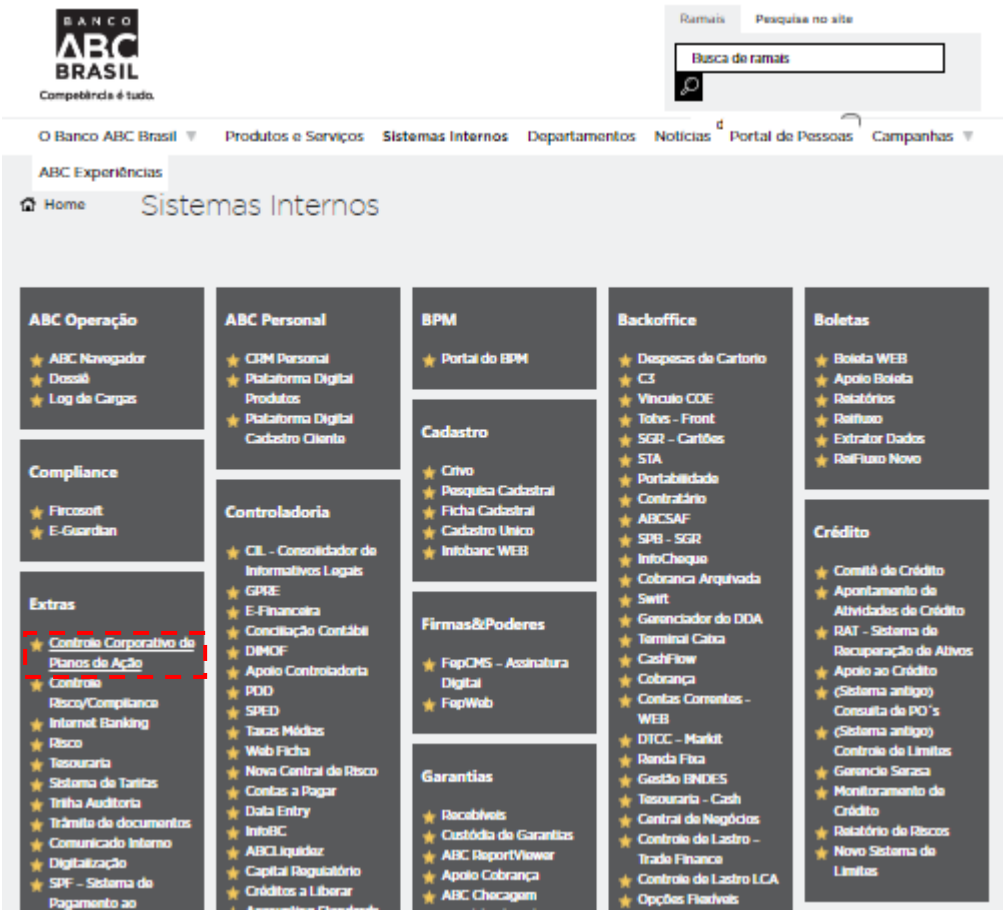
9.2. Controle Corporativo de Planos de Ação

A **DTVM** utiliza uma ferramenta interna de acompanhamento de planos de ação relacionados à gestão de riscos operacionais.

O aplicativo Controle Corporativo de Planos de Ação é a central para o registro e o acompanhamento de ações mitigatórias de riscos operacionais. Essa ferramenta permite o acesso dos gestores a todos os planos de ação de suas áreas e um acesso irrestrito da área de Gestão de Risco Operacional e Controle Interno e dos Vice-Presidentes ao seu conteúdo. O aplicativo também funciona como a base corporativa de planos de ação, registrando todo o histórico de planos em aberto, encerrados e cancelados.

O aplicativo Controle Corporativo de Planos de Ação possui acesso disponível na Intranet da **DTVM** , conforme abaixo:

FIGURA 7: APLICATIVO DE CONTROLE CORPORATIVO DE PLANOS DE AÇÃO

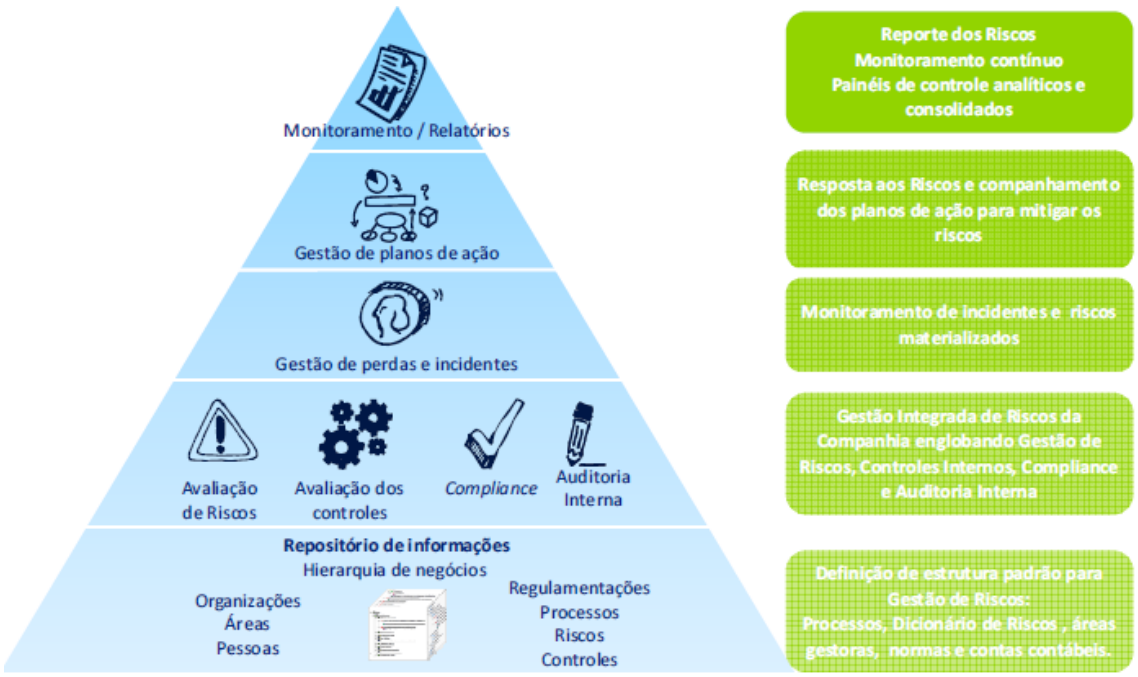


9.3. GRC BWise

A ferramenta GRC BWise é um sistema de Governança, Risco e Compliance fornecido pela empresa Nasdaq BWISE ao Grupo ABC em todo o mundo.

O GRC BWise oferece gerenciamento de riscos integrado, baseado em fluxos de trabalho, dos processos de Riscos Operacionais, Compliance e Auditoria Interna. Também inclui repositórios centrais para regulamentações, principais indicadores de risco, documentação de auditoria, incidentes de riscos operacionais e recursos para registrar e rastrear qualquer tipo de informação entre outros recursos.

FIGURA 8: GRC BWISE – FUNCIONALIDADES DA FERRAMENTA



Especificamente dentro da função de Gestão de Riscos Operacionais, os principais recursos disponíveis na ferramenta são:

- Fluxo de trabalho para gerenciamento de incidentes relacionados à riscos operacionais;
- Gerenciamento de banco de dados de perda;
- Manutenção e relatórios dos principais indicadores de risco (KRIs);
- Fluxo de trabalho para avaliações abertas e estruturadas;
- Fluxo de trabalho para avaliações (scans) de governança / estrutura.

10. Risco Operacional em Fornecedores Relevantes

O processo de avaliação de risco operacional em fornecedores relevantes foi implementado com o objetivo de monitorar o risco operacional decorrente de

serviços terceirizados relevantes para o funcionamento regular da instituição, em linha com os requerimentos da Resolução 4.557 do Banco Central do Brasil.

De acordo com o perfil de fornecedores mais acionado pela **DTVM** , definiu-se internamente como fornecedor 'relevante' todo fornecedor de serviços e produtos de tecnologia classificado como 'estratégico' pela área de Tecnologia – Infraestrura da **DTVM**.

Para todos os fornecedores classificados como fornecedor "estratégico" / "critico", é necessário o preenchimento de questionário para atendimento a Resolução 4.557 o qual está disponibilizado na requisição de compras na intranet corporativa.

Também em linha com os requerimentos da Resolução 4.557 do Banco Central do Brasil, no momento da contratação de um fornecedor relevante, é enviado ao fornecedor a Cartilha de Risco Operacional para Fornecedores e Terceiros (ver *Anexo 6*, com o objetivo de assegurar o adequado nivelamento de conhecimentos, boas práticas e expectativas da **DTVM** com relação ao contratado nos temas de gestão de risco operacional.

11. Risco Operacional em Novos Produtos, Processos e Sistemas

A área de Gestão de Risco Operacional e Controle Interno auxilia, quando acionado pelo ownerdo produto/serviço a elaboração de matriz de risco específica para o registro e acompanhamento dos riscos, controle e planos de ação para mitigação dos gaps identificados. A área de Gestão de Risco Operacional e Controle Interno participa do workfow de aprovação de novos produtos e serviços e é membro participante dos fóruns do Comitê de Produtos e do Grupo de Implementação.,

12. Capital Regulatório de Risco Operacional

Para o cálculo de seu Capital Regulatório de Risco Operacional, a **DTVM** aplica a "Abordagem Padronizada Alternativa", conforme definido na *Circular 3.640/13,* do Banco Central do Brasil.

O cálculo do Capital Regulatório de Risco Operacional, que usa como base dados de receita das linhas de negócio da **DTVM** , é atribuição da Vice-Presidência de

Finanças e Relações com Investidores, conforme politica interna *2540.ORG – Estrutura de Gestão de Capital*, sendo informado mensalmente para o Comitê Executivo.

13. Regulamentações e Referências

Regulatórios

- Resolução 4.893 do Banco Central do Brasil.
- Resolução 4.557 do Banco Central do Brasil.
- Resolução 4.968 do Banco Central do Brasil.
- Circular 3.640 do Banco Central do Brasil.
- Statement of Guidance Internal Controls Banks - Cayman Islands Monetary Authority (CIMA).

Boas Práticas

- Revisions to the Principles for the Sound Management of Operational Risk – BIS.
- Principles for the Sound Management of Operational Risk – BIS.
- Gerenciamento de Riscos Corporativos: Estrutura Integrada – COSO.