

	Política Corporativa	Código:	VFA-DCO-POL003
		Versão:	004
	Vice-Presidência Administrativa Financeira	Público alvo:	Geral
		Data da criação:	14/12/2017
	Política de Gestão de Riscos	Data da revisão:	03/08/2026
		Páginas:	1 / 10

SUMÁRIO

1.	OBJETIVO	2
2.	ABRANGÊNCIA	2
3.	REFERÊNCIAS	2
4.	SIGLAS E DEFINIÇÕES.....	2
5.	DIRETRIZES.....	3
6.	PROCESSO DE GESTÃO DE RISCOS	4
6.1.	ESTABELECIMENTO DO CONTEXTO	4
6.2.	IDENTIFICAÇÃO	5
6.3.	ANÁLISE DE RISCOS.....	5
6.4.	AVALIAÇÃO DE RISCOS.....	6
6.5.	TRATAMENTO DE RISCOS.....	7
6.6.	MONITORAMENTO DOS RISCOS	7
6.7.	COMUNICAÇÃO, REGISTRO E RELATO	8
7.	RESPONSABILIDADES.....	8
7.1.	DONO DO RISCO.....	8
7.2.	GERÊNCIA DE GESTÃO DE RISCOS	9
7.3.	COMITÊ DE AUDITORIA	10
7.4.	COMITÊ DE GESTÃO DE RISCOS (Órgão de Assessoramento a Diretoria)	10
7.5.	CONSELHO DE ADMINISTRAÇÃO	10
8.	RESPONSÁVEIS PELO DOCUMENTO	11
9.	REGISTRO DE ATUALIZAÇÕES	11

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	2 / 11

1. OBJETIVO

Estabelecer diretrizes e responsabilidades pertinentes ao processo de Gestão de Riscos, evidenciando a metodologia aplicada para os processos de identificação, avaliação, tratamento, monitoramento e comunicação dos riscos, inerentes ao negócio, incorporando a visão de riscos à tomada de decisões e ao planejamento estratégico, a fim de alinhar a governança da RD Saúde às boas práticas de mercado.

2. ABRANGÊNCIA

Este documento possui caráter corporativo e aplica-se a toda Companhia.

3. REFERÊNCIAS

- Código de Ética e Conduta da Raia Drogasil S.A.;
- Política de Anticorrupção, Antifraude e Relacionamento com Agentes Públicos;
- Política de Conflito de Interesse;
- Estatuto Social;
- Regimento Interno do Conselho de Administração;
- Regimento Interno do Comitê de Auditoria;
- Código da Gente;
- Regulamento do Novo Mercado;
- Resolução CVM 80;
- Ofício Circular da CVM SEP 01/17;
- COSO ERM (Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework);
- Publicações do IBGC - Instituto Brasileiro de Governança Corporativa;
- ISO (International Organization for Standardization) 31.000;
- IIA (The Institute of Internal Auditors).

4. SIGLAS E DEFINIÇÕES

- **Apetite a risco:** nível ao qual a Companhia está disposta a se expor em relação ao(s) risco(s) para cumprir seus objetivos estratégicos e agregar valor ao negócio.
- **Companhia:** Companhia e suas controladas.
- **Dono do risco:** área responsável por monitorar o risco que está sob sua tutela, bem como executar controles para mitigação dos riscos.
- **Fator de risco:** ocorrência de evento ou alteração de um conjunto específico de circunstâncias que contribuem para que eventualmente um risco se materialize. O mesmo risco pode conter um ou mais fatores relacionados.
- **Mapa de Riscos:** demonstração gráfica com base na análise geral dos riscos e de auto avaliação da Administração, em que são analisados os riscos da empresa, considerando impacto e probabilidade para sua materialização.

Uso Interno. Reprodução interna permitida, conforme versão na Intranet. Informações de propriedade do Grupo e não devem ser utilizadas, reproduzidas ou transmitidas externamente sem prévia autorização de seu proprietário.

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	3 / 11

- **Risco:** quaisquer eventos que, se materializados, podem impedir o alcance do propósito/ planejamento estratégico da Companhia. Abrange uma visão/ escopo de verificação da cadeia de forma integral, inclusive riscos e fatores de risco que podem estar associados a outros stakeholders.
- **Risco Inerente:** é o risco intrínseco à atividade exercida pela Companhia. São aqueles que a Companhia está exposta, desconsiderando as ações que possam reduzir sua probabilidade e/ ou impacto.
- **Risco Residual:** risco que permanece mesmo após a adoção de medidas utilizadas na mitigação do impacto e/ ou probabilidade de materialização do risco inerente.
- **Key Risk Indicator (KRIs):** principais Indicadores de Riscos, são componentes do processo de monitoramento de riscos, utilizados para fornecer indicadores antecipados ou atrasados de condições de risco em potencial.

5. DIRETRIZES

A Gestão de Riscos Corporativos está integrada ao processo de planejamento estratégico, orçamento e definição de iniciativas da Companhia, de modo a apoiar a tomada de decisões, a priorização de projetos e investimentos, bem como a avaliação de desempenho, considerando o nível de apetite a risco aprovado pela Alta Administração.

A Companhia identifica, avalia e monitora os riscos e seus fatores de risco, gerenciando com base no Modelo das Três Linhas, demonstrado pela figura abaixo:



Figura 1: O modelo das Três Linhas (adaptado de IIA)

Uso Interno. Reprodução interna permitida, conforme versão na Intranet. Informações de propriedade do Grupo e não devem ser utilizadas, reproduzidas ou transmitidas externamente sem prévia autorização de seu proprietário.

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	4 / 11

- 1ª linha (Áreas de Negócio ou Dono do Risco): São responsáveis por gerenciar os riscos de sua área, conduzir ações para mitigação dos riscos e ter propriedade sobre eles. Devem manter processos apropriados, garantindo a conformidade com as expectativas legais, regulatórias e éticas.
- 2ª linha (Gestão de Riscos e Controles Internos): Tem como objetivo apoiar a primeira linha, com expertise complementar incluindo a melhoria contínua das práticas de gestão de riscos nos níveis de processos e sistemas, fornecendo análises e reportando as adequações necessárias.
- 3ª linha (Auditoria Interna): Tem como objetivo uma avaliação objetiva e independente da gestão de riscos, identificando controles necessários a serem implementados. O Plano Anual de Auditoria Interna deve priorizar auditoria de processos com impacto em riscos mapeados, em especial os classificados como altos e muito altos.

6. PROCESSO DE GESTÃO DE RISCOS

O processo de Gestão de Riscos na Companhia é pautado em metodologias como ISO 31.000, COSO ERM, IBGC e IIA, sendo ordenado nas seguintes etapas:

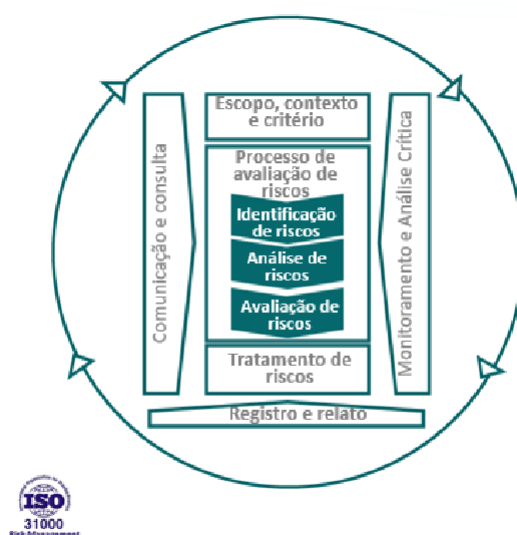


Figura 2: O Processo de Gestão de Riscos (ISO 31:000)

O processo da Gestão de Riscos está estruturado de acordo com as seguintes etapas, de forma a assegurar o cumprimento das diretrizes previstas nesta política:

6.1. ESTABELECIMENTO DO CONTEXTO

O estabelecimento do contexto é realizado pelo entendimento do ambiente interno, baseado no Planejamento Estratégico da Companhia e em seus objetivos e do ambiente externo, associados ao ambiente macroeconômico, político, social, natural e/ou setorial em que a Companhia opera.

Uso Interno. Reprodução interna permitida, conforme versão na Intranet. Informações de propriedade do Grupo e não devem ser utilizadas, reproduzidas ou transmitidas externamente sem prévia autorização de seu proprietário.

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	5 / 11

6.2. IDENTIFICAÇÃO

A etapa de identificação dos riscos é realizada por mapeamento de processos críticos da Companhia e reuniões de avaliações periódicas com os donos dos riscos, considerando a avaliação dos cenários internos e externos, bem como de resultados dos trabalhos de auditorias e controles internos.

O processo de gestão de riscos contempla também a identificação e avaliação de riscos emergentes, considerando tendências de mercado, transformações tecnológicas, regulatórias, ambientais e sociais. Entende-se por riscos emergentes aqueles que ainda não se manifestaram plenamente ou cuja materialidade e impacto estão em evolução, decorrentes de mudanças no ambiente externo ou interno, tais como transformações regulatórias, tecnológicas, sociais, ambientais, econômicas ou de mercado, que possam vir a afetar o alcance dos objetivos estratégicos da Companhia.

6.3. ANÁLISE DE RISCOS

A análise é realizada através dos riscos e seus fatores, descritos no dicionário de riscos da Companhia, classificados de acordo com a natureza identificada, sendo elas: Estratégico, Financeiro, Operacional, Conformidade e Tecnologia.

a) Detalhamento da Natureza dos Riscos:

- **Estratégico:** riscos que possam interromper o alcance de objetivos e a execução da estratégia planejada.
- **Financeiro:** riscos que afetem a estrutura de capital de maneira a comprometer a execução da estratégia da Companhia.
- **Operacional:** evento que possa interromper o alcance dos objetivos relacionados à operação do negócio, habitualmente decorrentes da inadequação ou falha nos processos internos e/ou pessoas.
- **Conformidade:** possibilidade de ocorrência de sanções em razão do descumprimento ou tratamento inadequado de normas externas (leis, regulamentos, recomendações e orientações de entidades reguladoras e auto-reguladoras, nacionais ou estrangeiras).
- **Tecnologia:** vulnerabilidades que possam impactar o negócio, como perdas financeiras decorrentes de ataques virtuais, ou mesmo de incidentes decorrentes de erros ou negligências causadas internamente na Companhia, que resultem em vazamento de dados e outros danos ligados ao sigilo da informação.

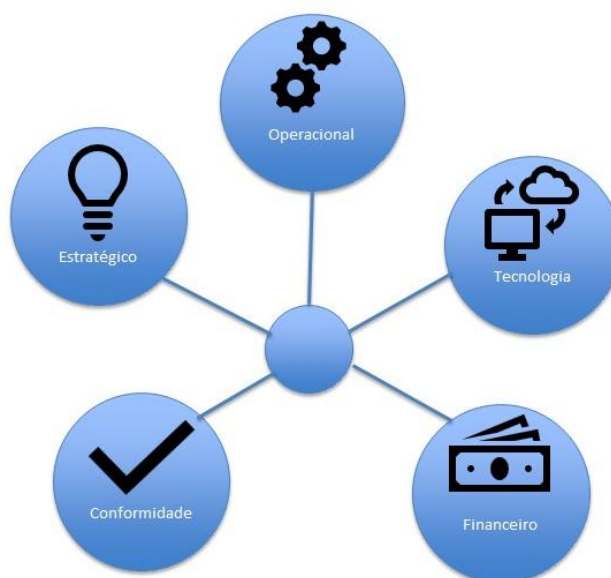


Figura 3: Natureza dos Riscos RD Saúde

6.4. AVALIAÇÃO DE RISCOS

A Companhia avalia os riscos identificados, utilizando como parâmetros o potencial impacto no negócio e a probabilidade de materialização dos riscos. Desta forma, a classificação é realizada através da combinação de impacto e probabilidade, conforme mapa de riscos definido pela Companhia:

		Probabilidade			
		Remoto	Possível	Provável	Muito Provável
Impacto	Muito Grave	Alto	Muito Alto	Muito Alto	Muito Alto
	Grave	Médio	Médio	Alto	Muito Alto
	Moderado	Baixo	Médio	Médio	Alto
	Leve	Baixo	Baixo	Médio	Médio

Figura 4: Mapa de Calor RD Saúde

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	7 / 11

- Impacto

São utilizados os critérios quantitativos (Financeiro) de acordo com o apetite a risco da Companhia e qualitativo (Imagem & Reputação, Operação e Regulatório), de acordo com os objetivos expressos no Planejamento Estratégico e os principais apontamentos de Negócio, de acordo com a gestão. O impacto do risco pode ser classificado em 4 escalas, sendo elas: Muito grave, Grave, Moderado e Leve.

- Probabilidade

Para compor a análise de probabilidade, são utilizados dados históricos e na existência de mitigadores (controles), como sendo os critérios para avaliação e classificação da possibilidade de materialização dos riscos. A probabilidade de materialização dos riscos pode ser classificada em quatro escalas: Muito provável, Provável, Possível e Remoto.

Importante: A avaliação dos riscos e seus fatores é realizada por parâmetros preestabelecidos (Impacto e Probabilidade), a fim de buscar transparência e equidade, evitando a subjetividade na classificação final dos riscos da companhia, não podendo ser alterada pelo dono do risco.

O detalhamento dos parâmetros definidos para a régua de Impacto e Probabilidade estão descritos no procedimento da área de Gestão de Riscos.

6.5. TRATAMENTO DE RISCOS

Após os riscos serem avaliados, é definido o tratamento a ser adotado considerando as seguintes ações:

- Reduzir: Implementar controles e planos de ações que possam diminuir as causas ou as consequências dos riscos.
- Compartilhar: Definir ações que visam reduzir a probabilidade de ocorrência e/ou impacto do risco, por meio da transferência ou compartilhamento total ou parcial do risco a terceiros, como, por exemplo, contratação de apólices de seguro, outsourcing, etc.
- Evitar: Estabelecer controles e planos de ações que visam eliminar a causa raiz do risco.
- Aceitar: A aceitação do risco pode ocorrer quando: i) se reconhece que a perda potencial de um risco não é suficientemente grande para justificar as possíveis ações mitigatórias; ii) em situações em que o custo da ação mitigatória ultrapasse a exposição ao risco; e iii) por estratégia do negócio. Para todas as situações descritas, é necessário a aprovação formal da instância de reporte (de acordo com a figura 5).

Para riscos classificados como graves ou muito graves, o tratamento poderá demandar a elaboração ou acionamento de planos específicos de continuidade de negócios, contingência e gestão de crises, assegurando a resiliência operacional e a adequada resposta a eventos disruptivos.

6.6. MONITORAMENTO DOS RISCOS

O monitoramento dos riscos da Companhia é realizado, sobretudo, pelo Comitê de Gestão de Riscos, órgão de assessoramento a Diretoria, no qual são estabelecidos encontros periódicos e específicos para acompanhamento dos riscos, de acordo com sua natureza. Essa fase contempla o acompanhamento dos controles e/ou indicadores- chave de riscos (KRIs), a evolução dos planos de ações definidos previamente pelos responsáveis pela condução dos respectivos riscos e a definição de novas ações para condução e/ou mitigação.

O monitoramento dos riscos da Companhia é realizado como pauta permanente do Comitê de Gestão de Riscos para os riscos muito altos e altos, os riscos médios e baixos são discutidos conforme necessidade. Adicionalmente, a Companhia mantém atividades contínuas de monitoramento, realizadas pela Gerência de Gestão de Riscos e avaliações independentes, realizadas pela área de Auditoria Interna ou empresas terceirizadas (auditoria externa).

A Companhia realiza também, com o envolvimento de sua Diretoria Executiva e Conselho de Administração, a revisão anual de seus riscos, para reavaliar o alinhamento à sua estratégia e verificação contínua da implementação e resultados das medidas mitigadoras.

De acordo com a sua exposição (combinação entre impacto e probabilidade), os riscos são reportados as instâncias aplicáveis, conforme o quadro a seguir:

Exposição ao Risco	Instância de Reporte	Alçada de Aceite ao Risco
Muito Alto	Conselho de Administração, Comitê de Auditoria e Comitê de Gestão de Riscos	Conselho de Administração
Alto	Conselho de Administração, Comitê de Auditoria e Comitê de Gestão de Riscos	CEO e VPs
Médio	Diretor	CEO e VPs
Baixo	Diretor	Diretor

Figura 5: Instância de Reporte dos Riscos

6.7. COMUNICAÇÃO, REGISTRO E RELATO

A Companhia divulga informações pertinentes às partes interessadas, em formato e prazo que possibilitem a execução das responsabilidades dos colaboradores, garantindo relevância, transparência, disponibilidade, acesso e exatidão das informações relativas a seus riscos. A área de Auditoria Interna pode realizar as auditorias nos processos a qualquer momento.

7. RESPONSABILIDADES

7.1. DONO DO RISCO

- Gerenciar risco sob sua responsabilidade, identificando alterações nos ambientes externos e internos que possam impactar os riscos e avaliando a necessidade de planos de ação para garantir seu tratamento.

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	9 / 11

- Implantar ações necessárias para a mitigação dos riscos, com o envolvimento de outras áreas, alinhadas ao plano de ação aprovado pela área de Gestão de Riscos.
- Realizar, periodicamente, revisão técnica do risco, dos fatores a ele relacionados, da resposta e da avaliação do risco, utilizando o conceito do Committee of Sponsoring Organizations of the Treadway Commission (COSO) para classificação dos principais riscos (probabilidade de ocorrência e impacto).
- Realizar reportes periódicos à área de Gestão de Riscos sobre a evolução dos riscos sob sua responsabilidade, mudanças significativas dos fatores de risco ou em qualquer outra característica do mesmo, ou identificação de novos riscos anteriormente não mapeados.
- Manter um efetivo ambiente de controle sob os riscos sob sua responsabilidade, evidenciando as ações implementadas.

7.2. GERÊNCIA DE GESTÃO DE RISCOS

- Disseminar o conhecimento sobre riscos e gestão de riscos aos funcionários, com o propósito de disseminar a cultura do gerenciamento de risco.
- Propor diretrizes da estrutura de governança corporativa de gestão de riscos da Companhia (metodologia, processos, sistemas, entre outros).
- Estabelecer e manter atualizados a Política de Gestão de Riscos, assim como padrões e mecanismos de reporte próprios de informações. Revisar e propor alterações nos procedimentos de gestão de riscos sempre que necessário.
- Assegurar que os gestores dos riscos identifiquem, mitiguem e monitorem os riscos da Companhia, bem como a integridade dos controles internos.
- Avaliar periodicamente os planos de ação, realizando testes e ajustes necessários, conforme reuniões com os gestores dos riscos, e estabelecendo prazos e responsáveis pela execução e reporte das ações mitigatórias.
- Aprimorar a metodologia do cálculo do apetite a risco, avaliando a probabilidade e o impacto dos riscos mapeados da Companhia.
- Colaborar, junto a Diretoria, Vice-Presidência, Presidência, Comitês de Gestão de Riscos, Comitê de Auditoria e Conselho de Administração, na discussão sobre a definição de apetite a risco aceitável da Companhia. Coordenar e monitorar o processo de identificação e avaliação dos riscos junto aos executivos da Companhia.
- Atualizar e revisar os fatores de risco periodicamente e sempre que houver atualizações no planejamento estratégico e/ou quando fatos relevantes ocorrerem.
- Manter atualizado o Mapa de Riscos da Companhia.
- Acompanhar e reportar mudanças na criticidade dos riscos no Comitê de Gestão de Riscos, Comitê de Auditoria e Conselho de Administração.
- Apresentar ao Comitê de Gestão de Riscos e Comitê de Auditoria os riscos a serem priorizados e os planos de ação propostos.
- Efetuar reportes periódicos ao Comitê de Gestão de Riscos e Comitê de Auditoria acerca do gerenciamento dos riscos.
- Avaliar o Mapa dos Riscos da companhia com uma visão independente, consolidada e integrada, bem como o apetite a riscos e recomendar ao Comitê de Auditoria ajustes e atualizações necessárias.

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	10 / 11

7.3. COMITÊ DE AUDITORIA

- Monitorar os riscos mapeados junto à Diretoria (estatutária e não-estatutária) e reportar periodicamente ao Conselho de Administração.
- Deliberar sobre o processo de gerenciamento de riscos (metodologia, processos, sistemas, política, mecanismos de reporte, dentre outros), solicitar ajustes, se necessário e recomendar ao Conselho de Administração.
- Reportar ao Conselho de Administração as exceções às diretrizes do processo de Gestão de Riscos e demais assuntos julgados relevantes.
- Acompanhar o planejamento da Gerência de Gestão de Riscos e solicitar ajustes se necessário, acompanhando a execução do trabalho e auferindo a qualidade e efetividade do processo, avaliar e monitorar as exposições e o gerenciamento dos riscos em geral da Companhia (e de sociedades investidas quando significarem potencial impacto para a Companhia).
- Avaliar e monitorar as exposições e o gerenciamento dos riscos da Companhia.
- Avaliar se a administração está adotando os controles necessários para o gerenciamento dos riscos.

7.4. COMITÊ DE GESTÃO DE RISCOS (Órgão de Assessoramento a Diretoria)

- Disseminar a cultura de gerenciamento de riscos visando assegurar o estrito cumprimento a todas as leis, normas e regulamentos a ela aplicáveis.
- Supervisionar os processos de gerenciamento dos riscos inerentes às atividades da Companhia e de suas controladas.
- Avaliar e monitorar as exposições de risco da Companhia.
- Propor e discutir procedimentos e sistemas de mensuração, gestão e o apetite à risco.
- Assegurar que as ações da Companhia são consistentes com o nível de riscos previamente determinados, bem como acompanhar periodicamente esse nível ou delegar a outro órgão da estrutura organizacional que faça tal acompanhamento.
- Assegurar que a Política de Gestão de Riscos e a estratégia de gerenciamento de riscos adotada pela Companhia reflitam a visão da Companhia.
- Revisar e acompanhar, periodicamente, o endereçamento dos apontamentos efetuados pela Gerência de Gestão de Riscos, bem como das auditorias interna/ externa, reguladores e Comitê de Auditoria.
- Manifestar-se sempre que identificar riscos emergentes e/ou aumento relevante na exposição a riscos existentes, recomendando sua inclusão na Matriz de Riscos Corporativos.

7.5. CONSELHO DE ADMINISTRAÇÃO

- Aprovar o nível de apetite e a classificação dos riscos (entre baixo, médio, alto e muito alto), com base na proposta apresentada pela Diretoria e validada pelo Comitê de Auditoria considerando combinação de impacto e probabilidade.
- Acompanhar os mecanismos de operacionalizações relacionadas à gestão de riscos, alinhando a coerência das políticas financeiras com as diretrizes estratégicas e o perfil de risco do negócio.

	Título: Política de Gestão de Riscos	Código:	VFA-DCO-POL003
		Páginas:	11 / 11

- Aprovar as diretrizes da estrutura de governança corporativa de gestão de riscos da Companhia (metodologia, políticas, processos, sistemas, entre outros), quando devidamente recomendados pelo Comitê de Auditoria.
- Acompanhar o cumprimento das metodologias estabelecidas, as ações mitigatórias e os planos de ação dos riscos inerentes, sobretudo que extrapolam o apetite ao risco da Companhia.
- Suportar as ações de conscientização dos gestores e colaboradores sobre a importância da gestão de riscos e a responsabilidade atribuída aos envolvidos no gerenciamento dos riscos da companhia.
- Assegurar a adequada gestão desta política, bem como a efetividade e a continuidade de sua aplicação.

8. RESPONSÁVEIS PELO DOCUMENTO

Responsável	Versão	Área	Cargo
Elaboração	4	Gerência de Gestão de Riscos	Gerente
Aprovação	4	Controladoria	Diretor
Aprovação	4	Conselho de Administração	Conselho

9. REGISTRO DE ATUALIZAÇÕES

Versão	Data Criação	Data Aprovação	Acesso	Manutenção Atualização	Armazenamento	Alterações
1	14/12/2017	14/12/2017	Corporativo	GRC	Conexão RD	N/A
2	18/08/2020	30/03/2021	Corporativo	GRC	Conexão RD	N/A
3	25/05/2022	29/07/2022	Geral	GRC	Workplace	N/A
3	25/05/2022	17/05/2024	Geral	GRC	Workplace	Data de Revisão
4	15/04/2026		Geral	GRC	Biblioteca do Conhecimento	Atualização Metodologia

Uso Interno. Reprodução interna permitida, conforme versão na Intranet. Informações de propriedade do Grupo e não devem ser utilizadas, reproduzidas ou transmitidas externamente sem prévia autorização de seu proprietário.