warren
Investimentos

ESTRUTURA DE RISCO OPERACIONAL, CONFORMIDADE, IMAGEM E LEGAL

001 COIN	Políticas da Instituição Controles Internos

Título	
002	**Estrutura de Risco Operacional, Conformidade, Imagem e Legal**

Instrumento Normativo Mandatório		
■ Política	☐ Norma	☐ Manual de Controles Internos | Procedimentos

Controle de Aprovação	
Aprovado pela Diretoria Executiva em: 08/08/2024	Válido até: 08/08/2025

* *Visando ao controle das revisões realizadas, as referidas devem ser registradas na última página do documento*.

Sumário

1. Objetivo

Estabelecer as regras que garantam a Gestão dos Riscos Operacional, de Conformidade, de Imagem e Legal, mantendo o permanente atendimento às políticas internas e regulamentações vigentes, a condução à compreensão dos principais riscos decorrentes de fatores internos e externos incorridos pelo Grupo Warren ("Warren").

A Gestão do Risco consiste na identificação, avaliação, mensuração, no monitoramento, controle e reporte dos riscos inerentes à atividade da Instituição.

2. Aplicação

As regras estabelecidas neste documento devem ser cumpridas pelos dirigentes, colaboradores, prestadores de serviços (“Colaboradores” / “Colaborador”) e parceiros externos vinculados ao Grupo Warren.

3. Implementação

Imediata, a partir da publicação na *Warrenpedia*.

4. Regra(s) Regulamentar(es)

- Resolução CVM nº 35, de 26 de maio de 2021: Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários e revoga a Deliberação CVM nº 105, de 22 de janeiro de 1991, e as Instruções CVM nº 51, de 9 de junho de 1986, CVM nº 333, de 6 de abril de 2000, CVM nº 505, de 27 de setembro de 2011, Instrução CVM nº 526, de 21 de setembro de 2012; Instrução CVM nº 581, de 29 de setembro de 2016; Instrução CVM nº 612, de 21 de agosto de 2019; e Instrução CVM nº 618, de 28 de janeiro de 2020.

- Resolução nº 4.595, de 28 de agosto de 2017: Dispõe sobre a política de conformidade (*compliance*) das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

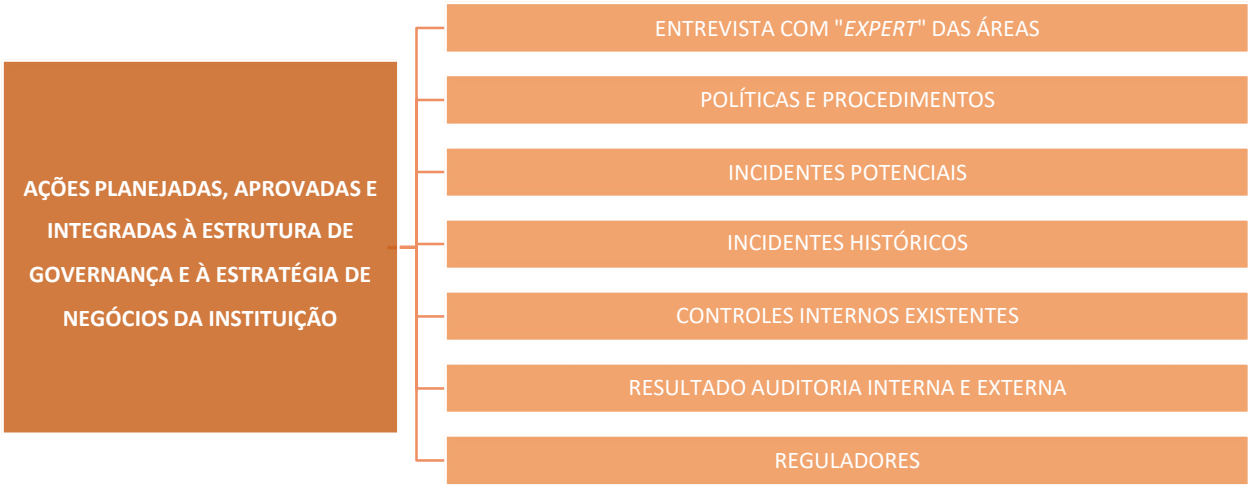
- Resolução Nº 4.943, de 15 de setembro de 2021: Altera a Resolução nº 4.557, de 23 de fevereiro de 2017, que dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

- Lei nº 12.846, de 01 de agosto de 2013 - Lei Anticorrupção: Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências.

- Resolução CMN Nº 4.968, de 25 de novembro de 2021: Dispõe sobre os sistemas de controles internos das instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

5. Diretrizes Gerais

A Diretoria de *Compliance*, Controles Internos e Auditoria atua, tempestivamente, para certificar que todas as ações planejadas e aprovadas estejam integradas à estrutura de governança e à estratégia de negócios da Instituição, garantindo o envolvimento da Diretoria Executiva, o monitoramento e o controle das exposições aos riscos, assegurando que estes estejam dentro dos limites definidos, visando à aderência às regras da Instituição e cumprindo com os requerimentos regulatórios.



5.1. Definição dos Riscos

Dentre os principais riscos do negócio estão o operacional, o de conformidade, o de imagem e o legal, os quais estão organizados de forma que proporcionem uma visão ainda mais clara sobre os esforços que devem ser empregados para atuar no gerenciamento de riscos da Instituição.

5.1.1. Risco Operacional

Resulta da possibilidade de perdas decorrentes de processos inadequados ou deficientes, erros, falhas nos sistemas de Tecnologia da Informação, problemas operacionais, fraudes, pessoas ou de ocorrências externas que ocasionem prejuízos às atividades ou danos aos ativos físicos da Instituição. Os eventos de Risco Operacional estão classificados em:

- Pessoas - Sistemas - Processos internos - Ocorrências externas	- Fraude interna - Fraude externa - Relações trabalhistas - Segurança deficiente do local de trabalho - Danos a ativos - Práticas inadequadas relativas a clientes e produtos - Situações acarretem a interrupção das atividades Falhas em sistemas - Falhas na execução, cumprimento de prazos e gerenciamento das atividades - Falhas em sistemas de tecnologia da informação	- Prejuízos - Obrigações legais - Ações regulatórias - Perda ou danos a ativos - Perdas de recursos - Danos à imagem - Exposição a outros riscos

Consequências

5.1.1.1. Principais Etapas do Processo de Riscos

Planejamento do gerenciamento dos riscos	· O primeiro passo é definir como o gerenciamento de riscos corporativos será feito. *Esta etapa deve ser sempre revisada e atualizada, corrigindo eventuais dificuldades identificadas durante a execução da gestão de riscos.*
Identificação dos riscos	· Identificar os riscos, documentar suas características e proceder análise de dados históricos e impactos.
Análise dos riscos	· Avaliar a exposição ao risco e proceder a priorização para ações; e · Efetuar a análise numérica do efeito dos riscos identificados.
Planejamento de respostas aos riscos	· Desenvolver ações para aumentar as oportunidades e reduzir as ameaças relacionadas; e · Desenvolver estratégias de respostas para os riscos e os planos de ações para cada um.
Implementação de respostas aos riscos	· Implementar as respostas planejadas em "Planejamento de respostas aos riscos" e os devidos planos de ação.
Monitoramento, Controle dos riscos e reporte	· Proceder o monitoramento dos riscos e o devido reporte. *Esta é a etapa em que os riscos identificados são acompanhados, além de ser o momento de identificar novos riscos, analisar a eficiência dos processos instaurados e implantar as ações corretivas necessárias após a análise.*

5.1.1.2. Nível de Risco | Resposta ao Risco

Ao analisar o risco, a área responsável deve estar consciente dos riscos relevantes que envolvem o negócio, bem como deve gerenciar esses riscos de forma que os objetivos estratégicos não venham a ser prejudicados. Assim, deve ser pré-requisito o estabelecimento

de objetivos estratégicos alinhados às determinações da Diretoria Executiva para que as áreas da Instituição procedam de forma conjunta e organizada.

Para cada risco identificado deve ser prevista uma resposta que pode ser: evitar, aceitar, compartilhar ou reduzir/mitigar. De acordo com, a metodologia utilizada pela Instituição, o COSO *(Committee of Sponsoring Organizations)*, sugere para cada resposta aplicada:

5.1.1.3. Respostas Aplicadas

Evitar	· Sugere que nenhuma opção de resposta tenha sido identificada para reduzir o impacto e a probabilidade a um nível aceitável. · Pode-se adotar a descontinuação das atividades que geram os riscos. Evitar riscos pode implicar a descontinuação de uma linha de produtos.
Reduzir (Mitigar)	· Diminui o risco residual a um nível compatível com as tolerâncias desejadas ao risco.
Compartilhar ou Transferir	· Uma ação é tomada para transferir ou compartilhar riscos em toda a Instituição ou com partes externas (conforme o caso, proceder a transferência do risco ao fornecedor).
Aceitar	· Indica que o risco inerente já esteja dentro das tolerâncias ao risco. *Aceitar o risco é uma forma de responder ao risco. Isso pode ocorrer, por exemplo, quando o custo de implementação de uma medida qualquer para responder a determinado risco fique muito alto, maior do que os benefícios trariam para a Instituição.*

5.1.1.4. Padrão Implementado – Nível de Risco | Resposta ao Risco | Critérios para Avaliação

Nível do Risco		Resposta ao Risco	
		Tipo	Ação
Risco Baixo	Indica que o nível de risco está dentro da tolerância ao risco.	Aceitar	Conviver com o evento, mantendo práticas e procedimentos de controle.
		Reduzir/Mitigar	Adotar medidas para reduzir a probabilidade ao impacto dos riscos.
Critérios para Avaliação (Impacto): - Perdas financeiras de pequena relevância; - Pagamentos de multas ou outras penalidades de pequena relevância.			

Nível do Risco		Resposta ao Risco	
		Tipo	Ação
Risco Médio	Indica que o nível de risco está próximo, mas não faz parte da tolerância ao risco.	Reduzir/Mitigar	Adotar medidas para reduzir a probabilidade ao impacto dos riscos.

Critérios para Avaliação (Impacto): - Perdas financeiras consideráveis; - Insatisfação de clientes; - Pagamentos de multas ou outras penalidades; - Perda de oportunidades de negócio; - Descumprimento de procedimentos internos, leis e regulamentações.

Nível do Risco		Resposta ao Risco	
		Tipo	Ação
Risco Alto	Indica que o nível de risco está fora da tolerância à riscos e deve ser reduzido a um nível compatível.	Reduzir/Mitigar	Adotar medidas para reduzir a probabilidade ao impacto dos riscos.
		Compartilhar/ Transferir	Reduzir a probabilidade - transferir/compartilhar uma parte do risco (por exemplo terceirização de atividade).
		Evitar	Promover ações que evitem ou atenuem de forma urgente as causas e/ou efeitos.
Critérios para Avaliação (Impacto): - Perdas financeiras significativas; - Perda de clientes ou de muitas transações; - Pagamento de multas elevadas ou penalidade severas; - Perda de grandes oportunidades de negócio ou investimentos.			

Nível do Risco		Resposta ao Risco	
		Tipo	Ação
Risco Muito Alto	Indica que o nível de risco está muito acima da tolerância a riscos. Neste caso as opções de respostas dificilmente devem reduzir a probabilidade e o impacto à níveis aceitáveis.	Reduzir/Mitigar	Adotar medidas para reduzir a probabilidade ao impacto dos riscos.
		Compartilhar/ Transferir	Reduzir a probabilidade - transferir/compartilhar uma parte do risco (por exemplo terceirização de atividade).
		Evitar	Promover ações que evitem ou atenuem de forma urgente as causas e/ou efeitos.
Critérios para Avaliação (Impacto): - Perdas financeiras que podem comprometer a rentabilidade do negócio; - Perda de clientes chave; - Pagamento de multas elevadas ou penalidades severas com impacto na imagem e reputação da Instituição; - Perda de grandes investimentos ou retorno muito abaixo do esperado.			

5.1.1.5. Prazo para o Tratamento dos Eventos de Risco Operacional

A Área de Controles Internos deve elaborar Planos de Ação em conjunto com as áreas envolvidas, com o objetivo de criar ou melhorar controles e/ou processos com o intuito de tratar os Eventos de Risco Operacional regitrados.

O prazo para o tratamento dos Eventos de Risco Operacional regitrados deve ser estipulado de acordo com o impacto a eles atribuidos.

O descumprimento do prazo determinado, pelas áreas envolvidas, será reportado à Diretoria de *Compliance*, Controles Internos e Auditoria para as providências cabíveis.

5.1.1.6. Acompanhamento dos Planos de Ação dos Eventos de Risco Operacional

O acompanhamento dos Planos de Ação dos Eventos de Risco Operacional deve ser realizado pela Área de Controles Internos, por meio de testes e/ou conferência.

O resultado obtido deve ser registrado e encaminhado ao envolvidos, inclusive à Diretoria de *Compliance*, Controles Internos e Auditoria.

Caso o resultado seja insatisfatório ou a implementação solicitada não tenha sido concluída no prazo determinado, deve ser registrado no Controle Interno: “em atraso”. É importante ressaltar que o prazo pré-determinado não será alterado.

5.1.1.7. Método de Atuação

A Estrutura de Controles Internos deve atuar de maneira integrada, registrando ocorrências e, respectivamente, as eventuais perdas operacionais incorridas. Deve realizar avaliações periódicas de suas atividades e processos, quando necessário, devendo implementar planos de ação para mitigar os riscos identificados, no intuito de aprimorar os controles e mecanismos que resultam em menor exposição aos riscos.

5.1.1.8. Implementação do Gerenciamento

Com a implementação, o Gerenciamento de Risco Operacional deve prever:

- A identificação, avaliação, o monitoramento, controle e a mitigação do risco;
- A documentação e o armazenamento de informações referentes às perdas associadas ao risco;
- A realização, com periodicidade mínima anual, de testes de avaliação dos sistemas de controles de riscos implementados;
- A existência de plano de contingência, contendo as estratégias a serem adotadas para assegurar condições de continuidade das atividades e para limitar graves perdas decorrentes de risco;
- A implementação, manutenção e divulgação de processo estruturado de comunicação e informação.

5.1.1.9. Processo

O Gerenciamento de Risco Operacional - em termos de direcionamento, implementação de novas iniciativas, e tomadas de decisões diárias, de forma contínua pertencendo a cada atividade operacional ou área. O objetivo de se reportar de forma unificada é estabelecer o processo de governança e hierarquia em que o gerenciador ou gestor seja completamente capaz de mensurar a exposição do risco operacional e tomar as devidas medidas corretivas rapidamente.

5.1.1.10. Causas de Risco Operacional

O Risco Operacional é constituído pela possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas, sistemas e eventos externos.

Processos Internos

– Falha ou falta de controle nos processos e/ou definição inadequada destes, conteúdo dos manuais internos e/ou das políticas desatualizados, procedimentos de segurança física ineficaz, concessão indevida de acessos aos sistemas.

Pessoas

– Relacionam-se à competência, desempenho das suas atribuições e conduta ética (quebra de sigilo de dados, discriminação, assédio, ações mal-intencionadas como fraudes e negociações escusas).

Sistemas

– Sistemas inadequados, falhas na segurança (ataques cibernéticos), falha na atualização de *softwares*, problemas relacionados à infraestrutura e arquitetura de TI, armazenamento de dados, processamento e rede.

Eventos Externos

– Alterações no ambiente econômico e político que podem interromper as atividades da Instituição parcial ou totalmente, desastres naturais (tempestades, inundações, entre outros), ações intencionais executadas por terceiros para lesar a Instituição, como por exemplo: falsificações, furtos, atos de vandalismos e terrorismo.

5.1.1.11. Consequências Relacionadas aos Eventos de Risco Operacional

Perdas Financeiras

– Resultado negativo na receita ou no lucro da Instituição, devido à(s) ocorrência(s) de Risco Operacional identificada(s).

Repercussão Reputacional Desfavorável

– Resultado negativo relacionado à imagem da Instituição, afetando sua reputação perante os clientes, mercado financeiro, órgãos reguladores, fornecedores e demais partes relacionadas.

Consequências Indiretas

– São consequências negativas de difícil mensuração financeira ou de gastos decorrentes de ações tomadas em função de algum evento ocorrido.

5.1.1.12. Elaboração de Relatório

Mediante a verificação de ocorrência, será desenvolvido um relatório específico com informações relevantes, podendo neste caso, utilizar o Relatório de Controles Internos, e ser submetido à Diretoria de *Compliance*, Controles Internos e Auditoria, que deve manifestar-se expressamente acerca das ações a serem implementadas para das deficiências apontadas.

5.1.2. Risco de Conformidade

Possibilidade de perdas financeiras ou de reputação resultantes de falha no cumprimento e/ou na observância do arcabouço legal, das regulamentações, das recomendações dos órgãos reguladores ou autorreguladores, dos códigos de conduta e ética, das diretrizes estabelecidas para o negócio e atividades da Instituição.

O monitoramento do Risco de Conformidade está sob a responsabilidade da Área de *Compliance,* que acompanha todos os processos da Instituição.

A Área de *Compliance* deve proceder de acordo com o determinado nos Itens abaixo, informados nesta Política, visando à análise e execução dos procedimentos necessários.

- Principais Etapas do Processo de Riscos;
- Nível de Risco | Resposta ao Risco;
- Padrão Implementado – Nível de Risco | Resposta ao Risco | Critérios para Avaliação; e
- Elaboração de Relatório (relacionado ao Risco de Conformidade).

5.1.3. Risco de Imagem

O Risco de Imagem, também conhecido como Risco Reputacional, representa a possibilidade de perda decorrente da deterioração da credibilidade ou reputação por mau desempenho do dever, de práticas antiéticas, da divulgação de informações negativas e de falha na comunicação interna ou externa.

O Risco de Imagem causa prejuízos aos valores da Instituição e envolve a percepção dos *stakeholders* (clientes, fornecedores, órgãos reguladores e demais partes interessadas), afetando a capacidade em estabelecer novas relações, acarretando impactos negativos na percepção da marca, expondo a Instituição a possíveis perdas financeiras ou uma redução na base de clientes.

O monitoramento do Risco Legal está sob a responsabilidade da Área de *Compliance,* que acompanha todos os processos da Instituição.

A Área de *Compliance* deve proceder de acordo com o determinado nos Itens abaixo, informados nesta Política, visando à análise e execução dos procedimentos necessários.

- Principais Etapas do Processo de Riscos;
- Nível de Risco | Resposta ao Risco;
- Padrão Implementado – Nível de Risco | Resposta ao Risco | Critérios para Avaliação; e
- Elaboração de Relatório (relacionado ao Risco de Imagem).

5.1.4. Risco Legal

Possibilidade de perda decorrente da inadequação ou deficiência em contratos firmados pela Instituição, bem como a sanções em razão do descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Instituição. Fazem parte, também, não conformidades com aspectos legais que envolvam produtos, contratos firmados e obrigações regulatórias, trabalhistas, fiscais, societárias, comerciais, cíveis e penais, dentre outras.

O monitoramento do Risco Legal está sob a responsabilidade da Área de *Compliance* que acompanha todos os processos da Instituição.

A Área de *Compliance* deve proceder de acordo com o determinado nos Itens abaixo, informados nesta Política, visando à análise e execução dos procedimentos necessários:

- Principais Etapas do Processo de Riscos;
- Nível de Risco | Resposta ao Risco;
- Padrão Implementado – Nível de Risco | Resposta ao Risco | Critérios para Avaliação; e
- Elaboração de Relatório (relacionado ao Risco Legal).

5.2. Apetite ao Risco

O apetite ao risco refere-se aos níveis e aos tipos de riscos que a Warren está disposta a admitir considerando a realização das operações.

Compete à Diretoria de *Compliance*, Controles Internos e Auditoria atribuir níveis de apetite aos riscos e revisá-los.

Com a atribuição dos níveis de apetite aos riscos, deve-se determinar as responsabilidades no gerenciamento operacional de riscos e nas execuções das atividades de controle, considerando ações para mitigações, regulamentares que disciplinam o processo de reporte à Diretoria de *Compliance*, Controles Internos e Auditoria, quando da verificação de violações dos processos de controles e dos limites de risco estabelecidos.

5.3. Disseminação da Cultura do Gerenciamento Contínuo do Risco Operacional e Continuidade de Negócios

Todos os Colaboradores recém-admitidos, devem ter treinamento sobre os conceitos de conformidade, garantindo assim a disseminação dos conceitos relacionados ao Gerenciamento Contínuo da Informação.

5.4. Conformidade (*Compliance*)

5.4.1. Definições

- ***Compliance*** – vem do verbo em inglês "*to comply*", que significa cumprir, executar, satisfazer, realizar o que lhe foi imposto, isto é, *compliance* é estar em conformidade; é o dever de cumprir e fazer cumprir os regulamentos internos e externos impostos às atividades da instituição. Estar "em *compliance*" é estar em conformidade com leis e regulamentos internos e externos.

- **Risco de Conformidade *(Compliance)*** – é o risco de sanções legais ou regulamentares, perdas financeiras ou mesmo perdas reputacionais decorrentes da falta de aderência a regulamentos, políticas e procedimentos internos e externos. O acompanhamento das atividades para atendimento às leis e regulamentos deve assegurar a conformidade no atendimento dos prazos e dos objetivos da Instituição, bem como deve ser gerenciado em conjunto com os demais riscos.

- **Conformidade regulatória** – é a aderência dos regulamentos internos em relação aos regulamentos externos.

- **Conformidade operacional** – é a aderência dos procedimentos e rotinas das dependências em relação aos regulamentos internos.

- **Não-conformidade** – é o não atendimento ou falta de cumprimento tempestivo das disposições legais e regulamentares nos processos operacionais.

5.4.2. *Compliance* Com Valor Agregado

A Warren compreende, por meio de seus valores, a importância das atividades de *Compliance,* não apenas como exigência regulatória, mas também como área de valor agregado, contribuindo positivamente nas estratégias adotadas e na qualidade na prestação de serviços.

5.4.3. Independência

Na estrutura organizacional da Warren, a Diretoria de *Compliance*, Controles Internos e Auditoria encontra-se subordinada à Diretoria Executiva. Portanto, está desvinculada das demais áreas submetidas à sua atuação, garantindo a independência para realização de suas atividades de forma imparcial e evitando possíveis conflitos de interesses, principalmente com as áreas de negócios da Instituição.

Embora trabalhem em conjunto, é mantida uma independência entre as atividades de gestão de riscos e auditoria interna, onde cada uma age de forma segregada e não subordinada uma à outra.

5.4.4. Acesso às Informações

Os responsáveis por atividades relacionadas à função de conformidade (*compliance*) devem ter livre acesso às informações necessárias para o exercício de suas atribuições.

A Diretoria Executiva deve prover estrutura de *compliance* e controles internos compatível com o porte da Instituição e meios necessários para que as atividades relacionadas à função de conformidade (*compliance*) sejam exercidas adequadamente.

5.4.5. Canal de Comunicação

A Diretoria de *Compliance*, Controles Internos e Auditoria deve possuir canais diretos de comunicação com a Alta Administração para o relato dos resultados de possíveis irregularidades ou falhas identificadas no decorrer das atividades.

5.4.6. Gerenciamento do Risco de Conformidade

O gerenciamento do risco de conformidade deve ocorrer de forma integrada com os demais riscos incorridos pela Warren, utilizando-se de metodologia própria que contempla as seguintes etapas:

1. **Identificação:** mapear de forma contínua os processos, a fim de assegurar a identificação de eventuais não conformidades que possam afetar os negócios e a reputação da Warren.

2. **Mensuração:** avaliar a aderência de forma sistemática, com base em planos de ação e testes de conformidade, para reportar tempestivamente eventuais falhas de não conformidades à Alta Administração.

3. **Monitoração/Mitigação:** adotar periodicamente critérios e mecanismos de controle de forma disciplinada, planejada e documentada, de modo a permitir o acompanhamento da exposição a riscos, estabelecendo planos de trabalho e ações para mitigá-los e/ou reduzir seu impacto na Warren.

5.4.7. Arquivamento

Os dados, registros e informações relativas aos mecanismos de controle, processos, testes e trilhas de auditoria devem ser mantidos à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos.

5.5. Regras Específicas

A Warren, entendendo a importância da segurança da informação, possui regras específicas que visam proteger os ativos de tecnologia e os dados dos seus clientes. Deste modo, toda

atividade desempenhada na Instituição, bem como a ela relacionada, deverá respeitar os princípios estabelecidos nas Políticas informadas a seguir:

- Regras associadas à proteção das informações e da propriedade intelectual estão estabelecidas na Política de Segurança da Informação – Corporativa.

- Regras referentes à proteção lógica da informação da Instituição e relacionadas especificamente às Diretorias e Áreas de TI estão estabelecidas na Política de Segurança da Informação – TI.

- Regras pertencentes à Segurança Cibernética, acessos às informações sensíveis de clientes e parceiros, estão determinadas na Política de Segurança Cibernética. A Instituição entende que a segurança cibernética se refere a um conjunto de práticas que protege a informação armazenada nos computadores e aparelhos de computação, sendo transmitida por meio das redes de comunicação, incluindo a *internet* e telefones celulares.

5.6. Sigilo, Segurança da Informação, Privacidade e Proteção de Dados

A Warren observa e cumpre toda a legislação aplicável à segurança da informação, privacidade e proteção de dados, inclusive (sempre e quando aplicáveis) à Constituição Federal, ao Código de Defesa do Consumidor, Código Civil, Marco Civil da Internet (Lei Federal nº 12.965/2014) e seu decreto regulamentador (Decreto 8.771/2016), à Lei Complementar nº 105/2001 (Lei do Sigilo Bancário), à Lei Complementar nº 166/2019 (altera a LC 105/2001), à Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados - "LGPD"), à Lei nº 13.853/2019 (altera a LGPD) e demais normas setoriais ou gerais sobre o tema. Para tanto, adota as medidas necessárias para garantir a confiabilidade de qualquer colaborador a ela vinculado, que venha a ter acesso aos dados pessoais coletados e tratados no âmbito do relacionamento com clientes, garantindo que o acesso esteja estritamente limitado àqueles que de fato precisam fazê-lo, de forma sigilosa e confidencial e em observância às disposições da LGPD e demais normas aplicáveis ao tema.

Em caso de armazenamento de dados pessoais e/ou dados sensíveis relacionados aos clientes, a Warren respeitará os padrões adequados de segurança, sigilo e confidencialidade, ficando o referido processo sujeito às auditorias regulatórias.

A LGPD conceitua "dados pessoais" e "dados sensíveis", ficando tais conceitos definidos como sendo (i) "dados pessoais": informações relacionadas à pessoa natural identificada ou identificável; e (ii) "dados sensíveis": dado pessoal passível de discriminação, tais como: origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

No âmbito do relacionamento com os clientes, a Warren estabelecerá controles de governança técnicos e administrativos internos que garantam a integridade e disponibilidade dos dados pessoais tratados, além de garantir a conformidade com a LGPD e demais normas aplicáveis ao tema.

6. Conformidade

6.1. Lei Anticorrupção e Confidencialidade das Informações

A Warren pauta suas atividades agindo com integridade e honestidade em suas práticas gerenciais e em suas operações comerciais, combatendo a corrupção e o suborno em todas as suas formas, especialmente por meio de seus colaboradores, fornecedores, terceiros e administradores. Desta forma, é vital para a Instituição que todos os mencionados tenham

conhecimento e observem todas as normas relacionadas à anticorrupção e suborno, sobretudo a Lei nº 12.846, de 01 de agosto de 2013 (“Lei Anticorrupção”).

Informações relacionadas às negociações e aos sistemas da Warren deverão ser mantidas de forma confidencial, inclusive em virtude da possibilidade de acesso remoto dos colaboradores às referidas informações. Portanto, todo cuidado deve ser tomado quanto ao que é dito, escrito ou comunicado, inclusive, eletronicamente, mesmo que em ambiente de trabalho remoto.

Neste ínterim, todos os Colaboradores deverão proteger as informações relacionadas às atividades da Instituição, devendo empregar o máximo dever de sigilo quanto aos dados obtidos em virtude, inclusive, mas não se limitando, aos acessos remotos efetuados dentro do Programa *Home Office*.

Com vistas à manutenção de sua reputação, ao cumprimento da Lei Anticorrupção e à confidencialidade das informações, a Warren instituiu o Código de Ética e Conduta da Warren, cujo conteúdo deve ser amplamente divulgado e observado.

7. Exceção às Regras estabelecidas neste Instrumento Normativo

Em havendo qualquer exceção relacionada às regras e diretrizes estabelecidas nesta Política, esta deverá ser aprovada, em primeira instância, pela Diretoria Executiva – CEO e Diretoria de *Compliance*.

8. Versionamento

Versão:	Data de Revisão:	Histórico:
01	31/07/2023	Elaboração do Documento.
02	08/08/2024	Revisão anual do conteúdo.