

DOCUMENTO OFICIAL · TERCEIRO SETOR

POLÍTICA DE INTEGRIDADE E COMPLIANCE

# Política de Compliance e Canal de Denúncias

---

RW CONSULTORIA LTDA. · CNPJ 12.337.151/0001-19 · Versão 1.0  
Maio de 2026 · RW Consultoria & Veritas Magna

---

**POLÍTICA DE INTEGRIDADE E COMPLIANCE****POLÍTICA DE COMPLIANCE E CANAL DE DENÚNCIAS**

RW Consultoria &amp; Veritas Magna · Versão 1.0 · Maio de 2026

**1. OBJETIVO****Estabelecer diretrizes, responsabilidades e fluxos formais para:**

- Disponibilização e gestão do Canal de Denúncias
- Recebimento e tratamento de relatos
- Proteção de dados e evidências
- Investigação técnica
- Emissão de Relatórios de Compliance
- Restrição de acesso às informações sensíveis

**Aplicável às atividades de monitoramento e avaliação de projetos executados por OSCs no âmbito da Lei 13.019/2014 (MROSC).****2. FUNDAMENTAÇÃO NORMATIVA**

- Lei nº 13.019/2014 (MROSC)
- Decreto regulamentador aplicável ao ente concedente
- Lei nº 13.709/2018 (LGPD)
- Princípios de Governança, Integridade e Controle Interno
- Normas de auditoria aplicáveis (quando pertinentes)

**3. PRINCÍPIOS DO CANAL**

- 1. Anonimato garantido (salvo manifestação voluntária do denunciante)**
- 2. Confidencialidade absoluta**
- 3. Proibição de retaliação**
- 4. Rastreabilidade das apurações**
- 5. Segregação de funções**
- 6. Restrição de acesso por perfil**
- 7. Integridade e preservação de evidências**

---

## 4. ESTRUTURA DE GOVERNANÇA

### 4.1 Comitê de Compliance (RW + Veritas)

**Composição mínima:**

- 1 membro da RW
- 1 membro da Veritas
- 1 membro suplente

**Responsabilidades:**

- Recebimento e triagem inicial
- Classificação de risco
- Deliberação sobre abertura de investigação
- Aprovação do Relatório Final de Compliance

## 5. FLUXO OPERACIONAL DO CANAL DE DENÚNCIAS

FLUXO OPERACIONAL

### FLUXO 1 — DISPONIBILIZAÇÃO DO CANAL

#### 5.1 Plataforma

O canal deverá:

- Ser hospedado em ambiente seguro (HTTPS)
- Permitir envio anônimo
- Não registrar IP automaticamente
- Possuir aviso de confidencialidade
- Conter política de tratamento de dados visível

#### 5.2 Divulgação

O canal será:

- Divulgado nos projetos monitorados
- Inserido em relatórios técnicos
- Disponibilizado às OSCs contratantes
- Informado em reuniões técnicas

FLUXO OPERACIONAL

### FLUXO 2 — RECEBIMENTO E FORMALIZAÇÃO DA DENÚNCIA

#### 5.3 Registro Automático

Ao receber denúncia:

1. Geração de número único de protocolo
  2. Registro em planilha ou sistema interno restrito
-

---

**3. Classificação preliminar por tipo:**

- o Desvio de recursos
- o Não execução de meta
- o Irregularidade contratual
- o Assédio / conduta inadequada
- o Fraude documental
- o Outro

**5.4 Formalização****O Comitê:**

- Analisa admissibilidade
- Classifica risco (baixo, médio, alto, crítico)
- Decide por:
  - o Arquivamento fundamentado
  - o Pedido de complementação
  - o Abertura de Procedimento Interno de Apuração (PIA)

**Prazo máximo para triagem: 5 dias úteis**

**FLUXO OPERACIONAL****FLUXO 3 — TRATAMENTO DE DADOS (LGPD)****5.5 Base Legal****Tratamento fundamentado em:**

- Exercício regular de direito
- Cumprimento de obrigação legal
- Legítimo interesse (com teste de proporcionalidade)

**5.6 Princípios Aplicados**

- Minimização de dados
- Necessidade
- Finalidade específica
- Segurança da informação
- Restrição de acesso

**5.7 Controle de Acesso****Acesso restrito exclusivamente a:**

- Membros designados da RW
- Membros designados da Veritas
- Sob termo formal de confidencialidade

---

**Proibido:**

- Compartilhamento informal
- Armazenamento em dispositivos pessoais
- Impressão sem autorização formal

**FLUXO OPERACIONAL****FLUXO 4 — ARMAZENAMENTO DE PROVAS****5.8 Provas Digitais****Devem ser:**

- Armazenadas em pasta criptografada
- Com controle de acesso por login individual
- Com registro de logs de acesso
- Nomeadas por número de protocolo

**5.9 Cadeia de Custódia****Para cada documento:**

- Registro de recebimento
- Registro de quem acessou
- Registro de alterações (se houver)

**Arquivos não podem ser editados — apenas duplicados para análise.**

**FLUXO OPERACIONAL****FLUXO 5 — INVESTIGAÇÃO E APURAÇÃO****5.10 Abertura do PIA****Documento formal contendo:**

- Número do protocolo
- Objeto da apuração
- Escopo
- Responsáveis pela apuração
- Cronograma

**5.11 Procedimentos de Apuração****Podem incluir:**

- Análise documental
  - Cruzamento financeiro
  - Conciliação com extratos
  - Entrevistas técnicas
  - Solicitação de esclarecimentos à OSC
-

- 
- Visita in loco

## 5.12 Prazo

**Prazo padrão: 30 dias Prorrogável mediante justificativa formal.**

FLUXO OPERACIONAL

## FLUXO 6 — RELATÓRIO DE COMPLIANCE

### 5.13 Estrutura do Relatório

#### 1. Identificação do Protocolo

#### 2. Síntese da denúncia

#### 3. Metodologia de apuração

#### 4. Evidências analisadas

#### 5. Achados técnicos

#### 6. Enquadramento normativo (Lei 13.019)

#### 7. Conclusão

#### 8. Recomendações:

- o Correção administrativa
- o Plano de ação
- o Comunicação ao ente público
- o Arquivamento

### 5.14 Classificação Final

- Procedente
- Parcialmente procedente
- Improcedente
- Inconclusiva

**Relatório aprovado pelo Comitê de Compliance.**

FLUXO OPERACIONAL

## FLUXO 7 — COMUNICAÇÃO E MEDIDAS

**Dependendo do caso:**

- Comunicação à OSC
- Comunicação ao órgão concedente
- Sugestão de instauração de tomada de contas
- Recomendação de glosa

- Plano de conformidade corretiva

## 6. RESTRIÇÃO DE ACESSO

### 6.1 Controle por Perfil

| Perfil               | Acesso                   |
|----------------------|--------------------------|
| Comitê de Compliance | Total                    |
| Analista designado   | Apenas casos atribuídos  |
| Diretoria            | Apenas relatórios finais |
| Terceiros            | Nenhum acesso            |

## 7. PRAZOS DE RETENÇÃO

Denúncias e evidências devem ser mantidas por:

- 5 anos após encerramento do projeto ou
- Prazo superior exigido pelo ente público

Após prazo legal → descarte seguro.

## 8. PROIBIÇÃO DE RETALIAÇÃO

É vedada qualquer forma de retaliação contra denunciante de boa-fé.

Caso identificada retaliação:

- Novo procedimento interno será instaurado.

## 9. MATRIZ RESUMIDA DOS FLUXOS

| Etapas       | Responsável        | Prazo    |
|--------------|--------------------|----------|
| Recebimento  | Sistema            | Imediato |
| Triagem      | Comitê             | 5 dias   |
| Investigação | Analista designado | 30 dias  |
| Relatório    | Comitê             | 10 dias  |
| Comunicação  | Diretoria          | 5 dias   |

## 10. INTEGRAÇÃO COM O MROSC

Este canal:

- Não substitui controle do ente público

- 
- Não substitui dever de prestação de contas
  - Atua como mecanismo preventivo e corretivo
  - Integra sistema de governança dos projetos monitorados

---

# MANUAL DE COMPLIANCE E GESTÃO DO CANAL DE DENÚNCIAS

RW Consultoria & Veritas Magna Versão 1.0

## CAPÍTULO I

### DISPOSIÇÕES GERAIS

#### Art. 1º – Finalidade

O presente Manual estabelece normas, procedimentos, fluxos operacionais e responsabilidades relativas ao Sistema de Compliance e ao Canal de Denúncias mantido conjuntamente pela RW Consultoria e pela Veritas Magna, no âmbito das atividades de monitoramento, auditoria técnica e acompanhamento de parcerias regidas pela Lei nº 13.019/2014.

#### Art. 2º – Âmbito de Aplicação

Este Manual aplica-se:

I – Às atividades internas da RW e Veritas; II – Aos projetos monitorados por ambas as empresas; III – Às denúncias relacionadas à execução física, financeira ou documental de parcerias firmadas sob o regime do MROSC.

#### Art. 3º – Fundamentos Normativos

O presente Manual fundamenta-se em:

- I – Lei nº 13.019/2014;
- II – Lei nº 13.709/2018 (LGPD);
- III – Regulamentos do ente concedente aplicável;
- IV – Princípios de governança, integridade e controle interno.

## CAPÍTULO II

### PRINCÍPIOS DO SISTEMA DE COMPLIANCE

#### Art. 4º – Princípios Estruturantes

O Sistema de Compliance observará os seguintes princípios:

- I – Confidencialidade;
- II – Garantia de anonimato;
- III – Proibição de retaliação;
- IV – Segregação de funções;
- V – Rastreabilidade das apurações;
- VI – Restrição de acesso por perfil;
- VII – Integridade e preservação de evidências.

---

**CAPÍTULO III**

## DO CANAL DE DENÚNCIAS

### Art. 5º – Natureza do Canal

O Canal de Denúncias constitui mecanismo formal, independente e confidencial para recebimento de relatos sobre:

- I – Desvio ou má aplicação de recursos;
- II – Descumprimento de metas;
- III – Irregularidades contratuais;
- IV – Fraude documental;
- V – Conflito de interesses;
- VI – Outras não conformidades relacionadas aos projetos monitorados.

### Art. 6º – Características Técnicas

O Canal deverá:

- I – Permitir envio anônimo;
- II – Operar em ambiente seguro (protocolo HTTPS);
- III – Não registrar IP automaticamente;
- IV – Exibir aviso de confidencialidade;
- V – Conter política de tratamento de dados visível ao usuário.

**CAPÍTULO IV**

## DA GOVERNANÇA E RESPONSABILIDADES

### Art. 7º – Comitê de Compliance

Fica instituído o Comitê de Compliance, composto por:

- I – Um representante da RW;
- II – Um representante da Veritas;
- III – Um suplente.

### Art. 8º – Competências do Comitê

Compete ao Comitê:

- I – Realizar triagem inicial das denúncias;
- II – Classificar o nível de risco;
- III – Deliberar sobre abertura de Procedimento Interno de Apuração (PIA);
- IV – Aprovar relatórios finais de compliance;
- V – Determinar medidas corretivas.

---

**CAPÍTULO V**

## **DO RECEBIMENTO E TRIAGEM**

### **Art. 9º – Registro da Denúncia**

Toda denúncia recebida deverá:

- I – Gerar número único de protocolo;
- II – Ser registrada em sistema interno restrito;
- III – Ser classificada preliminarmente por natureza e risco.

### **Art. 10 – Prazo de Triagem**

A triagem deverá ocorrer no prazo máximo de 5 (cinco) dias úteis, contados do recebimento.

### **Art. 11 – Decisão de Admissibilidade**

O Comitê poderá deliberar por:

- I – Arquivamento fundamentado;
- II – Solicitação de complementação;
- III – Instauração de Procedimento Interno de Apuração.

**CAPÍTULO VI**

## **DO TRATAMENTO DE DADOS PESSOAIS**

### **Art. 12 – Base Legal**

O tratamento de dados pessoais ocorrerá com fundamento em:

- I – Cumprimento de obrigação legal;
- II – Exercício regular de direitos;
- III – Legítimo interesse, observado teste de proporcionalidade.

### **Art. 13 – Medidas de Segurança**

Deverão ser observadas:

- I – Minimização de dados;
- II – Restrição de acesso por perfil;
- III – Armazenamento em ambiente seguro;
- IV – Proibição de uso de dispositivos pessoais;
- V – Registro de logs de acesso.

---

**CAPÍTULO VII**

## DO ARMAZENAMENTO E PRESERVAÇÃO DE PROVAS

### Art. 14 – Armazenamento

As evidências deverão ser:

- I – Armazenadas em pasta criptografada;
- II – Identificadas pelo número do protocolo;
- III – Mantidas com controle de acesso individualizado.

### Art. 15 – Cadeia de Custódia

Cada documento deverá possuir:

- I – Registro de recebimento;
- II – Registro de acesso;
- III – Registro de eventual duplicação para análise.

**CAPÍTULO VIII**

## DO PROCEDIMENTO INTERNO DE APURAÇÃO (PIA)

### Art. 16 – Instauração

O PIA será formalizado mediante documento contendo:

- I – Número do protocolo;
- II – Objeto da apuração;
- III – Escopo;
- IV – Responsáveis;
- V – Cronograma.

### Art. 17 – Prazo

O prazo padrão para conclusão será de 30 (trinta) dias, prorrogável mediante justificativa formal.

### Art. 18 – Métodos de Apuração

Poderão ser utilizados:

- I – Análise documental;
- II – Conciliação financeira;
- III – Entrevistas;
- IV – Solicitação formal de esclarecimentos;
- V – Visitas técnicas.

## CAPÍTULO IX

## DO RELATÓRIO DE COMPLIANCE

**Art. 19 – Estrutura**

O Relatório Final deverá conter:

- I – Identificação do protocolo;
- II – Síntese da denúncia;
- III – Metodologia;
- IV – Evidências analisadas;
- V – Achados técnicos;
- VI – Enquadramento normativo;
- VII – Conclusão;
- VIII – Recomendações.

**Art. 20 – Classificação**

O resultado poderá ser:

- I – Procedente;
- II – Parcialmente procedente;
- III – Improcedente;
- IV – Inconclusivo.

## CAPÍTULO X

## DA RESTRIÇÃO DE ACESSO

**Art. 21 – Perfis de Acesso**

- I – Comitê: acesso integral;
- II – Analista designado: acesso apenas aos casos atribuídos;
- III – Diretoria: acesso restrito ao relatório final;
- IV – Terceiros: acesso vedado.

## CAPÍTULO XI

## DA RETENÇÃO E DESCARTE

**Art. 22 – Prazo de Retenção**

As denúncias e evidências permanecerão arquivadas por:

- I – 5 (cinco) anos após encerramento do projeto; ou II – Prazo superior exigido pelo ente concedente.

---

**Art. 23 – Descarte**

O descarte deverá ocorrer de forma segura e documentada.

**CAPÍTULO XII**

## DA PROIBIÇÃO DE RETALIAÇÃO

**Art. 24 – Vedação**

É vedada qualquer forma de retaliação contra denunciante de boa-fé.

A constatação de retaliação ensejará abertura de novo procedimento interno.

**CAPÍTULO XIII**

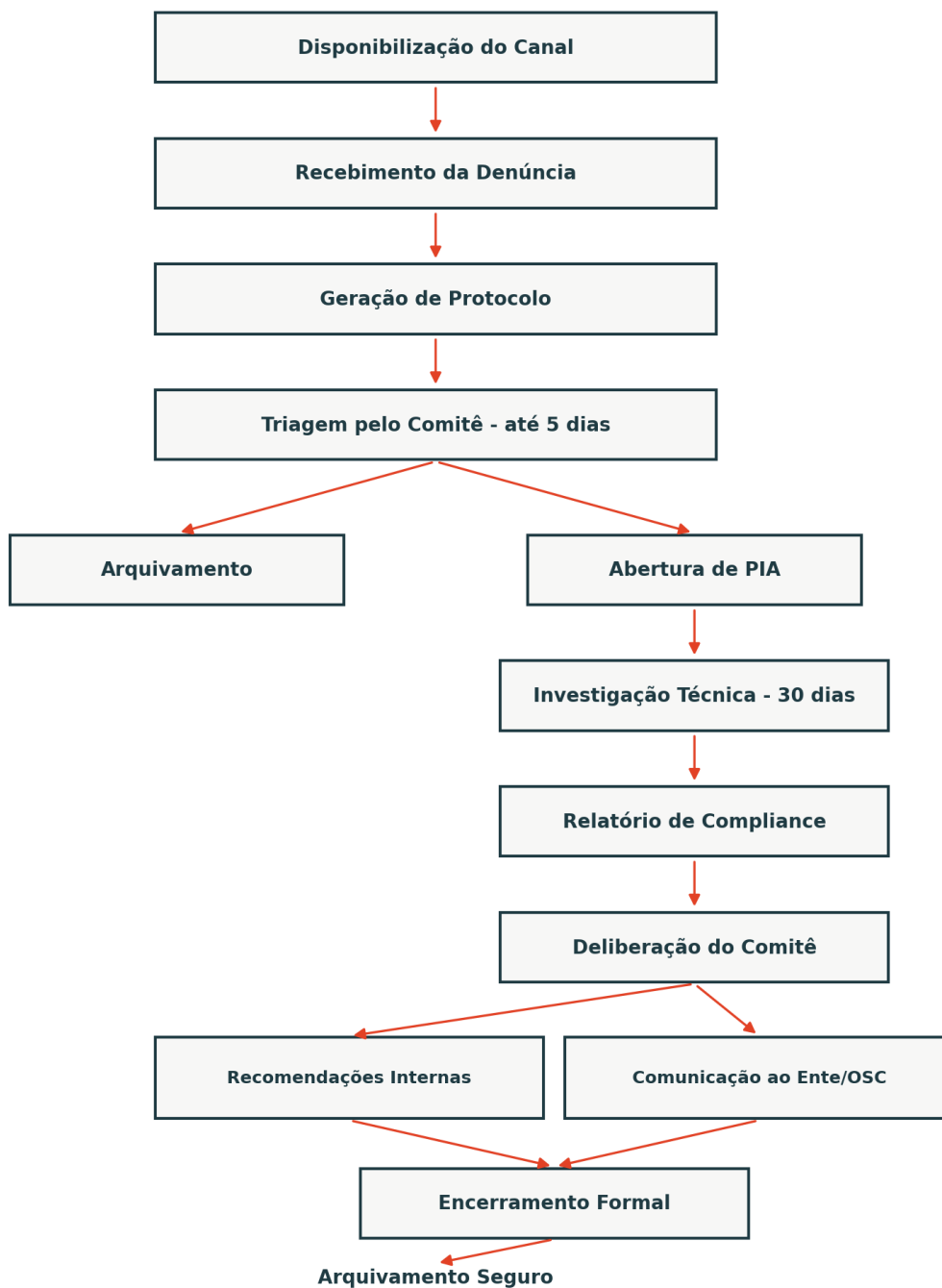
## DISPOSIÇÕES FINAIS

**Art. 25 – Revisão**

Este Manual poderá ser revisado mediante deliberação conjunta da RW e Veritas.

**Art. 26 – Vigência**

Entra em vigor na data de sua aprovação formal pelas Diretorias.



## ANEXO I

# MODELO DE INSTAURAÇÃO DE PROCEDIMENTO INTERNO DE APURAÇÃO (PIA)

## PROCEDIMENTO INTERNO DE APURAÇÃO – PIA Nº /

### 1. Identificação do Protocolo

o Nº do Protocolo da Denúncia:

o Data de Recebimento:

o Projeto Envolvido:

o OSC Envolvida:

### 2. Objeto da Apuração

(Descrição objetiva da denúncia)

### 3. Enquadramento Inicial

- ☐ Desvio de recursos
- ☐ Irregularidade documental
- ☐ Descumprimento de metas
- ☐ Fraude
- ☐ Conflito de interesses
- ☐ Outro:

### 4. Classificação de Risco

- ☐ Baixo
- ☐ Médio
- ☐ Alto
- ☐ Crítico

### 5. Designação

Analista Responsável:

Prazo para conclusão:

Data limite:

### 6. Escopo da Apuração

(Definir limites e metodologia)

### 7. Determinações Iniciais

- ☐ Solicitação de documentos
- ☐ Análise financeira
- ☐ Entrevistas
- ☐ Visita técnica

---

☐ Outras:

**8. Deliberação do Comitê**

Data:

Assinaturas:

---

**ANEXO II**

# MODELO DE RELATÓRIO FINAL DE COMPLIANCE

## RELATÓRIO DE COMPLIANCE Nº /

### 1. Identificação

o Nº do Protocolo:

o Nº do PIA:

o Projeto:

o OSC:

o Período analisado:

### 2. Síntese da Denúncia

(Descrição objetiva)

### 3. Metodologia Utilizada

o Análise documental

o Conciliação financeira

o Entrevistas

o Inspeção in loco

o Outros

### 4. Evidências Analisadas

(Listagem objetiva com identificação)

### 5. Achados Técnicos

(Descrição fundamentada)

### 6. Enquadramento Normativo

o Lei 13.019/2014

o Plano de Trabalho

o Instrumento Jurídico

o Regulamento aplicável

### 7. Conclusão

☐ Procedente

☐ Parcialmente procedente

☐ Improcedente

☐ Inconclusivo

### 8. Recomendações

☐ Plano corretivo

☐ Ajuste documental

---

☐ Comunicação ao ente público

☐ Sugestão de glosa

☐ Arquivamento

### **9. Aprovação do Comitê**

Data:

Assinaturas:

---

**ANEXO III**

## **MODELO DE ATA DE DELIBERAÇÃO DO COMITÊ**

### **ATA DE DELIBERAÇÃO – COMITÊ DE COMPLIANCE**

Data:

Local (ou virtual):

Presentes:

- Representante RW
- Representante Veritas
- Suplente (se aplicável)

Ordem do Dia:

Análise do Relatório de Compliance nº \_\_\_\_

Deliberação:

- ☐ Aprovação integral
- ☐ Aprovação com ajustes
- ☐ Determinação de diligência complementar
- ☐ Arquivamento

Fundamentação da decisão:

Encaminhamentos:

Encerramento às \_\_\_\_.

Assinaturas:

---

**ANEXO IV**

## **MODELO DE TERMO DE CONFIDENCIALIDADE**

### **TERMO DE CONFIDENCIALIDADE – COMPLIANCE**

Eu, \_\_\_\_\_, declaro que:

- 1. Terei acesso a informações sensíveis relacionadas a denúncias.**
- 2. Comprometo-me a manter absoluto sigilo.**
- 3. Não compartilharei informações com terceiros não autorizados.**
- 4. Não utilizarei dispositivos pessoais para armazenamento.**
- 5. Estou ciente das sanções internas e legais em caso de violação.**

Local e data:

Assinatura:

## ANEXO V

## MATRIZ DE CLASSIFICAÇÃO DE RISCO

| Critério             | Baixo             | Médio    | Alto        | Crítico          |
|----------------------|-------------------|----------|-------------|------------------|
| Valor envolvido      | Até 1% do projeto | Até 5%   | Até 15%     | >15%             |
| Impacto reputacional | Local             | Regional | Municipal   | Estadual/Federal |
| Risco jurídico       | Baixo             | Moderado | Elevado     | Imediato         |
| Evidência preliminar | Frágil            | Parcial  | Consistente | Robusta          |

Classificação final: média ponderada dos critérios.

## ANEXO VI

## MODELO DE PLANO DE CONFORMIDADE CORRETIVA

### PLANO DE CONFORMIDADE CORRETIVA

Protocolo: Projeto: OSC:

Irregularidade Identificada:

Medidas Corretivas:

| Ação | Responsável | Prazo | Indicador de Verificação |
|------|-------------|-------|--------------------------|
|      |             |       |                          |

Prazo de Monitoramento:

Acompanhamento:

Assinaturas:

## ANEXO VII

## CONTROLE DE CADEIA DE CUSTÓDIA

| Nº Protocolo | Documento | Data Recebimento | Responsável | Forma de Armazenamento | Acessos Registrados |
|--------------|-----------|------------------|-------------|------------------------|---------------------|
|              |           |                  |             |                        |                     |

## ESTRUTURA CONSOLIDADA DOS ANEXOS

I – Instauração de PIA

II – Relatório Final

III – Ata de Deliberação

IV – Termo de Confidencialidade

V – Matriz de Risco

VI – Plano Corretivo

VII – Cadeia de Custódia

---

# PROCEDIMENTO OPERACIONAL PADRÃO (POP)

## PROCEDIMENTO OPERACIONAL

### SISTEMA DE COMPLIANCE E CANAL DE DENÚNCIAS

RW Consultoria & Veritas Magna Código: POP-COMP-01 Versão: 1.0

## 1. OBJETIVO

Padronizar as etapas operacionais relacionadas ao recebimento, apuração e tratamento de denúncias vinculadas aos projetos monitorados no âmbito da Lei 13.019/2014.

## 2. ABRANGÊNCIA

Aplica-se a:

- Comitê de Compliance
- Analistas designados
- Diretoria RW e Veritas
- Área de Segurança da Informação

## 3. DEFINIÇÕES

Denúncia: Relato formal de possível irregularidade. PIA: Procedimento Interno de Apuração. Comitê: Órgão colegiado responsável por deliberação. Evidência: Documento, dado ou informação verificável.

## PROCEDIMENTO OPERACIONAL

### ETAPA 01 — DISPONIBILIZAÇÃO E MONITORAMENTO DO CANAL

#### Objetivo

Garantir funcionamento contínuo, seguro e rastreável do canal.

#### Responsável

Diretoria + Segurança da Informação

#### Entradas

Manual aprovado Configuração técnica da plataforma

#### Atividades

1. Verificar protocolo HTTPS ativo
2. Confirmar anonimato habilitado
3. Testar geração automática de protocolo
4. Validar aviso de confidencialidade
5. Registrar teste em ata

---

**Controle**

Checklist semestral de funcionamento

**Saída**

Canal validado e operacional

**PROCEDIMENTO OPERACIONAL****ETAPA 02 — RECEBIMENTO DA DENÚNCIA****Objetivo**

Formalizar o registro da denúncia.

**Responsável**

Sistema (automático) + Comitê

**Entradas**

Denúncia submetida

**Atividades**

1. Gerar número único de protocolo
2. Registrar data e hora
3. Classificar preliminarmente por natureza
4. Armazenar em banco restrito

**Controle**

Planilha/sistema com controle de acesso

**Saída**

Denúncia registrada formalmente

Prazo máximo para triagem: 5 dias úteis

**PROCEDIMENTO OPERACIONAL****ETAPA 03 — TRIAGEM E ADMISSIBILIDADE****Objetivo**

Determinar se a denúncia será apurada.

**Responsável**

Comitê de Compliance

**Entradas**

Registro da denúncia

**Atividades**

1. Analisar elementos mínimos
2. Avaliar pertinência ao escopo contratual
3. Classificar risco (baixo, médio, alto, crítico)
4. Deliberar:

- 
- Arquivamento fundamentado ou
  - Instauração de PIA

**Controle**

Ata de deliberação

**Saída**

Despacho formal

**PROCEDIMENTO OPERACIONAL****ETAPA 04 — INSTAURAÇÃO DO PIA****Objetivo**

Formalizar abertura da investigação.

**Responsável**

Comitê

**Entradas**

Deliberação de admissibilidade

**Atividades**

1. Preencher modelo de Instauração
2. Designar analista responsável
3. Definir prazo e escopo
4. Registrar no sistema interno

**Controle**

Documento PIA numerado

**Saída**

PIA formalmente instaurado

**PROCEDIMENTO OPERACIONAL****ETAPA 05 — COLETA E PRESERVAÇÃO DE EVIDÊNCIAS****Objetivo**

Garantir integridade e rastreabilidade das provas.

**Responsável**

Analista + Segurança da Informação

**Entradas**

Documentos recebidos

**Atividades**

1. Registrar evidência na cadeia de custódia
  2. Armazenar em pasta criptografada
  3. Restringir acesso por perfil
  4. Gerar log de acesso
-

---

5. Realizar backup seguro

**Controle**

Planilha de Cadeia de Custódia

**Saída**

Evidências preservadas

**PROCEDIMENTO OPERACIONAL****ETAPA 06 — ANÁLISE TÉCNICA****Objetivo**

Avaliar materialidade e conformidade.

**Responsável**

Analista designado

**Entradas**

Evidências coletadas

**Atividades**

1. Conciliação financeira
2. Verificação documental
3. Cruzamento com plano de trabalho
4. Análise jurídica (quando necessário)
5. Redação de achados técnicos

**Controle**

Checklist metodológico

**Saída**

Conclusão preliminar

Prazo padrão: 30 dias

**PROCEDIMENTO OPERACIONAL****ETAPA 07 — ELABORAÇÃO DO RELATÓRIO FINAL****Objetivo**

Formalizar resultado da apuração.

**Responsável**

Analista + Comitê

**Entradas**

Conclusão preliminar

**Atividades**

1. Redigir relatório conforme modelo
2. Indicar enquadramento normativo

---

3. Classificar resultado

4. Submeter ao Comitê

**Controle**

Assinatura do Comitê

**Saída**

Relatório Final aprovado

**PROCEDIMENTO OPERACIONAL****ETAPA 08 — DELIBERAÇÃO E MEDIDAS****Objetivo**

Determinar providências.

**Responsável**

Comitê + Diretoria

**Entradas**

Relatório aprovado

**Atividades**

1. Classificar resultado
2. Definir medidas corretivas
3. Elaborar ofício à OSC (se necessário)
4. Comunicar ente público (quando aplicável)
5. Definir prazo de cumprimento

**Controle**

Registro formal de comunicação

**Saída**

Encaminhamento formalizado

**PROCEDIMENTO OPERACIONAL****ETAPA 09 — MONITORAMENTO DO PLANO CORRETIVO****Objetivo**

Verificar implementação das medidas.

**Responsável**

Comitê

**Entradas**

Plano corretivo

**Atividades**

1. Acompanhar prazos
  2. Solicitar comprovação
  3. Avaliar eficácia
-

4. Registrar conclusão

#### Controle

Relatório de Monitoramento

#### Saída

Encerramento ou reabertura

#### PROCEDIMENTO OPERACIONAL

## ETAPA 10 — ENCERRAMENTO E ARQUIVAMENTO

#### Objetivo

Finalizar o processo com segurança jurídica.

#### Responsável

Compliance

#### Entradas

Caso concluído

#### Atividades

1. Classificar para retenção
2. Arquivar por 5 anos
3. Registrar data de descarte futuro
4. Garantir armazenamento seguro

#### Controle

Registro de retenção

#### Saída

Processo encerrado formalmente

## INDICADORES DE DESEMPENHO (KPIs)

| Indicador                       | Meta      |
|---------------------------------|-----------|
| Prazo médio de triagem          | ≤ 5 dias  |
| Prazo médio de investigação     | ≤ 30 dias |
| % denúncias concluídas no prazo | ≥ 90%     |
| Incidentes de vazamento         | 0         |

## MATRIZ RESUMIDA DE RESPONSABILIDADES

| Etapa       | Comitê | Analista | Diretoria | Segurança TI |
|-------------|--------|----------|-----------|--------------|
| Recebimento | ✓      |          |           |              |
| Triagem     | ✓      |          |           |              |

| Etapa              | Comitê | Analista | Diretoria | Segurança TI |
|--------------------|--------|----------|-----------|--------------|
| PIA                | ✓      |          |           |              |
| Investigação       |        | ✓        |           |              |
| Relatório          | ✓      | ✓        |           |              |
| Comunicação        | ✓      |          | ✓         |              |
| Segurança de Dados |        |          |           | ✓            |