2R DATATEL TELEINFORMÁTICA LTDA

CNPJ: 73.514.382/0001-45

Praça Quinze de Novembro, 20 — Sala 401B — Centro — Rio de Janeiro / RJ

PROGRAMA DE INTEGRIDADE

Versão 3.0 · Documento Institucional — Uso Restrito

Lei Anticorrupção 12.846/2013 · Decreto 11.129/2022 · Lei 14.133/2021 (NLLC) · LGPD ISO 37001 (Antissuborno) · ISO 27001 (SI) · ISO 9001 (Qualidade) · ISO 27701 (Privacidade)

Sumário

1. APRESENTAÇÃO E BASE NORMATIVA

A 2R Datatel Teleinformática Ltda é uma empresa especializada em Tecnologia da Informação, Cibersegurança, Serviços Especializados com 33 anos de atuação em todo o território nacional, sediada no Rio de Janeiro. Seus serviços principais — SOC as a Service 24×7, Managed Security Services (MSS) e a Plataforma Eskudo de cibersegurança — são prestados a clientes dos setores público e privado, incluindo órgãos da Administração Pública Federal, Estadual e Municipal.

A natureza dos serviços da 2R Datatel impõe responsabilidade de integridade de dupla ordem: como empresa que contrata com o Poder Público (sujeita à Lei Anticorrupção, à NLLC e ao Decreto 11.129/2022) e como custodiante de dados sensíveis de clientes — logs de segurança, eventos de rede, credenciais, informações de infraestrutura crítica — o que torna a integridade na gestão da informação inseparável da integridade ética e anticorrupção.

Este Programa de Integridade é o instrumento central de governança da 2R Datatel. Não é um documento declaratório — é um sistema operativo, com controles verificáveis, métricas, responsáveis nominados e mecanismos de aplicação. Foi concebido para atender simultaneamente aos requisitos do Decreto 11.129/2022 (parâmetros de avaliação de programas de integridade em contratações públicas), da ISO 37001 (Gestão Antissuborno) e das normas ISO 27001, 9001, 27701, 45001 e 14001, todas certificadas.

1.1 Base Legal e Normativa

Instrumento	Aplicação neste Programa
Lei 12.846/2013 — Anticorrupção	Responsabilidade objetiva da empresa por atos lesivos à Administração Pública. Base para vedações, controles e o canal de denúncias.
Decreto 11.129/2022	Regulamenta a Lei 12.846/2013 e define os parâmetros de avaliação de programas de integridade para fins de atenuação de sanções e qualificação em licitações.
Lei 14.133/2021 — NLLC	Nova Lei de Licitações e Contratos: due diligence de integridade como requisito de habilitação; integridade como critério de desempate; vedações específicas a conflito de interesses.
Lei 13.709/2018 — LGPD	Tratamento de dados pessoais de clientes, colaboradores e terceiros. Integrada à Seção 10 deste Programa.
ISO 37001:2018	Sistema de Gestão Antissuborno: avaliação de risco, due diligence, controles financeiros, declarações de conflito de interesse. Certificada.

ISO 27001:2022	Segurança da Informação: controles de acesso, gestão de incidentes, continuidade. Integrada como pilar de integridade na Seção 9.
ISO 9001:2015	Gestão da Qualidade: processos documentados, auditoria, melhoria contínua. Reforça a verificabilidade dos controles.
ISO 27701:2019	Extensão de privacidade da ISO 27001: requisitos de proteção de dados pessoais — base normativa da Seção 10.
ISO 45001:2018	Saúde e Segurança Ocupacional: ambiente de trabalho íntegro e seguro — base da Seção 11.
ISO 14001:2015	Gestão Ambiental: responsabilidade socioambiental como componente de governança.

2. MISSÃO, VISÃO, VALORES E CULTURA DE INTEGRIDADE

2.1 Missão

Fornecer soluções inovadoras e seguras de tecnologia da informação e cibersegurança, protegendo ativos digitais de clientes públicos e privados, promovendo eficiência operacional e impulsionando resultados com base em princípios éticos, técnicos e de conformidade inabaláveis.

2.2 Visão

Ser a referência em cibersegurança gerenciada no Brasil, reconhecida não apenas pela excelência técnica, mas pela integridade institucional que nos habilita a guardar o que nossos clientes têm de mais sensível: sua infraestrutura, seus dados e sua confiança.

2.3 Valores

Os valores da 2R Datatel não são aspiracionais — são critérios de tomada de decisão:

Valor	Como se manifesta na prática
Integridade sem negociação	Nenhuma oportunidade de negócio, pressão comercial ou interesse individual justifica violação ética, normativa ou legal.
Transparência ativa	Informações relevantes são compartilhadas proativamente com clientes, colaboradores e órgãos de controle — não apenas quando exigidas.
Segurança como responsabilidade	Somos custodiantes de dados críticos. Falhar na segurança é falhar na integridade. Os dois pilares são inseparáveis na 2R Datatel.
Conformidade como diferencial	Nossas certificações (ISO 37001, 27001, 9001) não são selos — são sistemas operantes com auditorias, controles e métricas verificáveis.

Responsabilidade com o Público	Contratar com a Administração Pública é um privilégio que exige controles adicionais e tolerância zero com irregularidades.
Diversidade e respeito	Um ambiente plural, seguro e inclusivo é pré-condição para decisões éticas de qualidade.
Melhoria contínua	Nenhum programa de integridade é definitivo. Aprendemos com incidentes, auditorias e feedbacks para melhorar continuamente.

3. COMPROMETIMENTO E RESPONSABILIDADE DA ALTA DIREÇÃO

O comprometimento da Alta Direção com a integridade não é retórico. Manifesta-se por atos concretos e verificáveis, que o Decreto 11.129/2022 (art. 56, §1º) exige como primeiro parâmetro de avaliação de um programa de integridade efetivo.

3.1 Atos de Comprometimento da Direção

Ato de Comprometimento	Evidência Verificável	Frequência
Aprovação formal e assinatura deste Programa	*Assinatura constante da última página deste documento*	A cada revisão
Participação nas reuniões do Comitê de Integridade	*Atas de reunião com presença da Direção registrada*	Trimestral (mínimo)
Comunicação pública do compromisso ético	*Carta do Diretor Presidente publicada e enviada a todos os colaboradores*	Anual
Alocação de recursos para o Programa	*Orçamento aprovado para treinamentos, ferramentas e auditorias externas*	Anual (ciclo orçamentário)
Revisão e aprovação das políticas vinculadas	*Aprovação formal das revisões das políticas do SGI vinculadas ao Programa*	Anual ou por evento
Declaração pessoal de conflito de interesses	*Formulário de DCi preenchido e assinado pela Direção*	Anual + eventos relevantes
Resposta pessoal a incidentes graves	*Participação direta na resposta a incidentes de integridade de alta gravidade*	Por evento
Tone at the top em licitações	*Comunicação direta do Diretor ao gestor comercial sobre vedações em contratações públicas*	Por processo licitatório

⚖ **FUNDAMENTO LEGAL Decreto** 11.129/2022, art. 56, §1º: o comprometimento da alta direção é o primeiro e mais relevante parâmetro de avaliação. Programas de integridade sem evidência concreta de envolvimento da direção são considerados "de papel" pelos órgãos de controle e pelo CGU.

4. ESTRUTURA DE GOVERNANÇA — COMITÊ DE INTEGRIDADE

A governança do Programa de Integridade é exercida pelo Comitê de Integridade (CI), órgão colegiado com autoridade, independência e acesso direto à Alta Direção, responsável por supervisionar, revisar e aprimorar continuamente o Programa.

4.1 Composição do Comitê de Integridade

Cargo / Função	Papel no Comitê
Coord. Qualidade / SGI — Auditor Interno	Presidir reuniões · Coordenar investigações · Gerir o canal de denúncias · Reportar à Direção · Manter documentação do Programa
CISO — Chief Information Security Officer	Representar o pilar de Segurança da Informação · Reportar incidentes de SI com implicação de integridade · Gerir due diligence técnica de terceiros
Diretor Comercial	Representar o pilar comercial · Supervisionar controles em processos licitatórios · Aprovar relacionamentos com agentes públicos e intermediários
Diretor Presidente	Participação obrigatória nas reuniões trimestrais · Aprovação de decisões de alta gravidade · Garantir recursos e autoridade ao CI
Data Protection Officer / Assessoria Jurídica	Representar o pilar de Privacidade e LGPD · Avaliar implicações legais de investigações · Orientar sobre obrigações regulatórias

4.2 Funcionamento e Alçadas

Parâmetro	Definição
Periodicidade	Reunião ordinária: trimestral. Reunião extraordinária: convocada em até 48h para incidentes de gravidade Alta ou Crítica, ou sempre que o Responsável pelo Programa julgar necessário.
Quórum	Mínimo: Presidente do CI + 2 membros. A presença do Diretor Presidente é obrigatória nas reuniões ordinárias.
Pauta mínima obrigatória	(a) Status das investigações abertas; (b) Indicadores do Programa; (c) Denúncias recebidas no período; (d) Incidentes de SI com implicação de integridade; (e) Due diligence de terceiros pendentes; (f) Deliberações sobre sanções ou encaminhamentos.

Atas	Lavradas em até 5 dias úteis após cada reunião. Assinadas por todos os presentes. Arquivadas no SGD por 5 anos.
Deliberações	Por maioria simples. Empate: voto de qualidade do Presidente do CI. Decisões sobre demissão ou comunicação a autoridades: aprovação do Diretor Presidente obrigatória.
Alçada — Advertência	Presidente do CI + 1 membro. Registro em ata.
Alçada — Suspensão ou restrição de acesso	Presidente do CI + Diretor Comercial ou CISO.
Alçada — Demissão por justa causa	Presidente do CI + Diretor Presidente. Parecer jurídico recomendado.
Alçada — Comunicação a autoridades (CGU, MP, TCU)	Presidente do CI + Diretor Presidente. Obrigatório quando há indício de ato lesivo à Administração Pública.
Independência	Membros do CI não sofrem retaliação por exercer suas funções. O Presidente do CI tem acesso direto ao Diretor Presidente e pode reportar ao Conselho ou a órgãos externos quando necessário.

5. CERTIFICAÇÕES E SISTEMA DE GESTÃO INTEGRADO (SGI)

As certificações da 2R Datatel não são ornamentais. Cada uma é um sistema operante com políticas, controles, auditorias internas e externas e ciclo de melhoria contínua documentado. Juntas, formam o Sistema de Gestão Integrado (SGI) que sustenta e evidencia o Programa de Integridade.

Norma	Sistema de Gestão	Contribuição para o Programa	Auditoria
ISO 37001:2018	SGAS — Antissuborno	Pilar central: due diligence de terceiros, avaliação de risco de suborno, declarações de conflito de interesse, controles financeiros.	Anual (interna + externa)
ISO 27001:2022	SGSI — Segurança da Informação	Proteção dos dados de clientes como obrigação de integridade. Controles de acesso, gestão de incidentes, CMDB, continuidade.	Anual (interna + externa)

ISO 9001:2015	SGQ — Qualidade	Processos documentados e verificáveis. Gestão de NCs. Rastreabilidade das ações do Programa.	Anual (interna + externa)
ISO 27701:2019	PIMS — Privacidade	Proteção de dados pessoais de clientes e colaboradores. Complementa LGPD. Base da Seção 10.	Anual (integrada à 27001)
ISO 45001:2018	SGSST — SSO	Ambiente de trabalho íntegro e seguro. Prevenção de assédio como componente de integridade.	Anual (interna + externa)
ISO 14001:2015	SGA — Ambiental	Responsabilidade socioambiental como componente de governança corporativa.	Anual (interna + externa)

🔑 **PONTO-CHAVE O** SGI da 2R Datatel documenta mais de sessenta (60) procedimentos, políticas e registros integrados às seis normas. O Programa de Integridade é parte formal deste SGI, garantindo que os controles de conformidade são auditáveis, rastreáveis e sujeitos ao ciclo PDCA de melhoria contínua.

6. CÓDIGO DE ÉTICA E CONDUTA EMPRESARIAL

O Código de Ética e Conduta Empresarial (CECE) é o instrumento que traduz os valores da 2R Datatel em regras de conduta concretas e verificáveis. Aplica-se a todos os colaboradores, estagiários, prestadores de serviço, parceiros e terceiros que atuem em nome da empresa.

6.1 Princípios de Conduta

Princípio	Regras Específicas
Conflito de interesses	(a) Declarar ao CI qualquer situação que possa influenciar decisões profissionais em benefício próprio ou de terceiros; (b) Abster-se de participar de decisões nas quais haja interesse pessoal; (c) Preencher e assinar o Formulário de Declaração de Conflito de Interesse (DCI) anualmente e sempre que surgir nova situação; (d) Vedado exercer atividade incompatível com as funções na 2R Datatel sem autorização prévia.
Presentes, brindes e hospitalidade	(a) Vedado oferecer ou receber presentes, brindes, viagens, entretenimento ou qualquer vantagem de agentes públicos ou privados que possa influenciar decisões; (b) Brindes institucionais de valor simbólico

	(≤ R$ 100,00) podem ser recebidos, desde que registrados; (c) Qualquer oferta acima deste valor: recusar e comunicar ao CI imediatamente.
Informações confidenciais	(a) Dados de clientes, logs de segurança, configurações de infraestrutura e informações de incidentes são confidenciais; (b) Proibido compartilhar com terceiros não autorizados, incluindo membros da família; (c) A violação de confidencialidade é ato de alta gravidade — ver Seção 15.
Uso de ativos e sistemas	(a) Ativos de TI da empresa são de uso profissional; uso pessoal incidental é tolerado desde que não comprometa segurança; (b) Proibido instalar software não autorizado, usar credenciais alheias ou acessar sistemas sem autorização; (c) O uso de IA é regulado pela POL-IA-01 — proibido submeter dados de clientes a ferramentas não homologadas.
Relacionamento com agentes públicos	(a) Todo contato substantivo com agente público relacionado a processos de contratação deve ser registrado; (b) Proibido oferecer qualquer vantagem a agente público, direta ou indiretamente; (c) Reuniões com agentes públicos em processos licitatórios devem ser formais, documentadas e, se possível, com presença de mais de um colaborador.
Anticoncorrência	(a) Proibido participar de conluio, cartel, combinação de propostas ou qualquer prática anticompetitiva; (b) Proibido trocar informações comercialmente sensíveis com concorrentes; (c) Dúvidas sobre a legalidade de uma prática: consultar o CI antes de prosseguir.
Mídias sociais e comunicação	(a) Proibido divulgar dados ou informações confidenciais de clientes em qualquer canal; (b) Manifestações em nome da 2R Datatel devem ser autorizadas pela Direção; (c) Opiniões pessoais em redes sociais não representam a empresa — identificar claramente.

i NOTA O CECE é disponibilizado a todos os colaboradores no ato da admissão e revisado anualmente. A leitura e ciência são formalizadas por assinatura de termo. Dúvidas sobre a aplicação das regras devem ser levadas ao Responsável pelo Programa antes da ação — nunca depois.

7. POLÍTICA ANTISSUBORNO E ANTICORRUPÇÃO (ISO 37001)

A 2R Datatel é certificada na ISO 37001 — Sistema de Gestão Antissuborno. Esta seção detalha os controles operacionais que sustentam essa certificação e que vão além da declaração de vedação: avaliação de risco, due diligence, controles financeiros e mecanismos de resposta.

🚫 **VEDAÇÃO ABSOLUTA**: é proibido oferecer, prometer, dar, solicitar, aceitar ou receber, direta ou indiretamente, qualquer vantagem indevida — financeira ou não financeira — a qualquer pessoa, pública ou privada, para obter ou manter negócios ou vantagem comercial indevida. Esta vedação aplica-se a colaboradores, intermediários, parceiros e qualquer terceiro que atue em nome da 2R Datatel.

7.1 Avaliação de Risco de Suborno

A avaliação de risco de suborno é realizada anualmente e sempre que houver mudança relevante de contexto (novo mercado, novo tipo de contrato, novo parceiro). Os fatores avaliados incluem:

Fator de Risco	Nível Atual	Controles Existentes	Responsável
Contratos com o setor público	🔴 Alto	Seção 8 completa — controles específicos	*Diretor Comercial + CI*
Uso de intermediários / representantes	🔴 Médio-Alto	Due diligence §7.2 + contrato com cláusula antissuborno	*CI + Diretor Comercial*
Processos de licitação	🔴 Alto	Seção 8 — controles de participação em licitações	*Diretor Comercial + CI*
Pagamentos a terceiros (parceiros, fornecedores)	🟠 Médio	Aprovação dupla + verificação CNPJ + contrato com cláusula antissuborno	*Financeiro + CI*
Patrocínios, doações e contribuições	🟠 Médio	Aprovação prévia do CI — proibido a agentes públicos	*CI + Direção*
Presentes e hospitalidade	🟠 Médio	Política de presentes §6.1 — limite R$100 + registro	*CI*

Acesso a dados de clientes públicos	🔴 Alto	ISO 27001 controles + SGI-NDA-COL-01 + monitoramento SOC	*CISO*

7.2 Due Diligence de Terceiros

Todo terceiro que possa expor a 2R Datatel a risco de suborno — intermediários, representantes comerciais, consultores de relacionamento governamental, fornecedores críticos — é submetido a due diligence antes da contratação e reavaliado anualmente.

	Item de Due Diligence	Como Verificar	Responsável	Bloqueio se
1	Verificação de CNPJ e situação cadastral	*Receita Federal + SINTEGRA + consulta CNPJ*	*Financeiro*	*CNPJ inativo ou irregular*
2	Pesquisa em listas restritivas (CEIS, CNEP, CEPIM)	*Portais CGU — consulta obrigatória*	*CI*	*Consta em qualquer lista*
3	Pesquisa de mídia negativa	*Busca estruturada em mídia + Google + DOU*	*CI*	*Indício de envolvimento em corrupção*
4	Verificação de vínculo com agentes públicos	*Declaração do terceiro + pesquisa pública*	*CI + Diretor Comercial*	*Parente de 1º grau de agente público decisor sem aprovação da Direção*
5	Verificação de processos judiciais e administrativos	*Consulta a tribunais + TJRJ + STJ + STF*	*CI / Jurídico*	*Condenação em atos de corrupção, improbidade ou lavagem*
6	Avaliação de reputação de mercado	*Referências comerciais + certificações + histórico*	*Diretor Comercial*	*Reputação incompatível com os valores da 2R Datatel*
7	Cláusula antissuborno no contrato	*Minuta contratual revisada por jurídico*	*Jurídico*	*Recusa em assinar cláusula — suspender contratação*
8	Declaração de ausência de conflito de interesse	*Formulário DCI assinado pelo terceiro*	*CI*	*Recusa em declarar*

7.3 Controles Financeiros Antissuborno

Controle	Descrição
Aprovação dupla para pagamentos acima de R$ 5.000	Todo pagamento acima deste valor exige aprovação de dois signatários autorizados. Pagamentos a agentes públicos ou seus familiares: aprovação do Diretor Presidente obrigatória.
Proibição de pagamentos em espécie	Todos os pagamentos são realizados via transferência bancária identificada. Vedado pagamento em espécie, criptomoedas não rastreáveis ou vales-presente.
Remuneração de intermediários baseada em critérios claros	Vedado pagar comissão ou honorários sem contrato formal, escopo definido, entregáveis verificáveis e due diligence aprovada.
Proibição de contas secretas ou registros falsos	Todo pagamento é registrado na contabilidade com sua finalidade real. Vedado registrar despesa com descrição diferente da real.
Revisão periódica de despesas de representação	O CI revisa semestralmente as despesas de hospitalidade, brindes e entretenimento para identificar padrões irregulares.
Vedação de doações a partidos e campanhas políticas	Proibido qualquer contribuição a partidos políticos, campanhas eleitorais ou candidatos, em qualquer forma.

8. CONTRATAÇÕES COM O SETOR PÚBLICO — CONTROLES ESPECÍFICOS

A prestação de serviços à Administração Pública Federal, Estadual e Municipal expõe a 2R Datatel a riscos específicos de integridade que exigem controles adicionais além dos aplicáveis a contratações privadas. Esta seção implementa as exigências do Decreto 11.129/2022 e da Lei 14.133/2021 para empresas que contratam com o Poder Público.

⚖ **FUNDAMENTO LEGAL Decreto** 11.129/2022, art. 55: a existência de programa de integridade estruturado é fator de atenuação de sanções por atos lesivos à Administração Pública (Lei 12.846/2013, art. 7º, inciso VIII). A robustez e efetividade do programa determinam o grau de atenuação — programas "de papel" não são considerados pelo CGU.

8.1 Controles na Participação em Processos Licitatórios

Controle	Procedimento Obrigatório
Verificação de impedimentos antes de participar	Consultar CEIS (Cadastro de Empresas Inidôneas e Suspensas), CNEP e CEPIM antes de cada processo. Resultado deve ser formalmente registrado. Empresa com registro: comunicar ao CI imediatamente.
Proibição de conluio e combinação de propostas	Proibido qualquer contato com concorrentes sobre valores, estratégias ou desistência de licitações. Qualquer aproximação deste tipo deve ser imediatamente reportada ao CI.
Controle de contato com a comissão de licitação	Todo contato com membros da comissão de licitação ou agentes públicos decisores deve ser formal (pelo sistema eletrônico), registrado e comunicado ao CI.
Vedação de pagamentos para vantagem em licitação	Proibido qualquer pagamento, presente, promessa ou vantagem a agente público ou privado que possa influenciar o resultado do processo.
Revisão ética da proposta pelo CI	Antes da assinatura de propostas em licitações de alto valor (≥ R$ 100.000,00), o CI deve revisar e aprovar a integridade do processo de elaboração.
Documentação completa do processo de participação	Todas as etapas da participação em licitações são documentadas: identificação da oportunidade, elaboração da proposta, contatos realizados, resultado. Retenção: 5 anos.
Declaração do colaborador responsável	O colaborador responsável pelo processo licitatório assina declaração de que não há irregularidade ética na participação.

8.2 Controles na Execução de Contratos Públicos

Controle	Procedimento
Registro de interações com agentes públicos	Todo contato substantivo (reuniões, negociações, solicitações fora do escopo contratual) com fiscais ou gestores do contrato deve ser registrado em log com: data, participantes, pauta e resultado.
Proibição de pagamentos fora do contrato	Vedado qualquer pagamento ou prestação de serviço a ente público além do que está formalmente contratado — mesmo que solicitado informalmente.
Gestão de subcontratados em contratos públicos	Subcontratados em contratos públicos passam pelo mesmo processo de due diligence (§7.2) e assina cláusula antissuborno equivalente.
Segregação de funções na execução	A pessoa que elabora a proposta não pode ser a mesma que autoriza pagamentos relacionados ao contrato. Revisão do CI para contratos ≥ R$ 200.000,00.
Relatório periódico de execução ao CI	Para contratos de longa duração (≥ 12 meses), o gestor do contrato apresenta relatório semestral ao CI sobre a execução e relacionamento com o órgão.
Protocolo de denúncia de irregularidade do cliente	Se a 2R Datatel identificar solicitação irregular de um agente público durante a execução: recusar, registrar e comunicar ao CI em até 24 horas. O CI avalia denúncia a órgãos de controle.

8.3 Habilitação e Integridade como Requisito na NLLC

A Lei 14.133/2021 introduziu novos requisitos de integridade relevantes para a 2R Datatel:

- Art. 60, §1º: empresas com programa de integridade têm vantagem em critérios de desempate — este Programa é o instrumento para fazer valer esse direito.
- Art. 155, I: improbidade ou condenação por atos anticorrupção é causa de inabilitação — o monitoramento das listas restritivas (§8.1) é o controle preventivo.
- Art. 94: o programa de integridade pode ser exigido como condição de habilitação em contratos de grande vulto — a 2R Datatel está preparada para atender essa exigência.
- Art. 25, §12: declaração de integridade deve ser apresentada na proposta — o CI certifica a regularidade antes de cada processo.

9. SEGURANÇA DA INFORMAÇÃO COMO PILAR DE INTEGRIDADE

Para a 2R Datatel, segurança da informação e integridade são inseparáveis. Somos custodiantes de dados altamente sensíveis de nossos clientes — logs de eventos de segurança, alertas de incidentes, configurações de infraestrutura crítica, dados de acesso privilegiado. O uso indevido dessas informações — mesmo que sem intenção financeira direta — constitui violação grave de integridade com potencial de dano irreversível.

9.1 Obrigações de Integridade na Gestão da Informação

Obrigação	Controles e Evidências
Confidencialidade de dados de clientes	SGI-NDA-COL-01 (NDA de colaboradores) + SGI-NDA-FORN-01 (NDA de fornecedores). Classificação de informação em 5 níveis (SGI-7.5-PCD-01 §3.3). Proibido compartilhar dados de clientes com terceiros não autorizados, incluindo outros clientes.
Controle de acesso privilegiado (PAM)	PAM implementado (CI-APP-PAM-001). Contas privilegiadas gerenciadas e auditadas. Revisão semestral de acessos (CSI-SI-01). Princípio do menor privilégio aplicado. Logs de acesso retidos por 12 meses.
Vedação ao uso de dados de clientes para fins próprios	Proibido usar qualquer informação obtida no escopo dos serviços SOC/MSS para benefício próprio, de terceiros ou de concorrentes. Violação: demissão por justa causa + ação civil.
Gestão de incidentes com implicação de integridade	Incidentes P1/P2 que envolvam dados de clientes são reportados ao CI em ≤ 2h (além do fluxo SOC). CI avalia obrigação de notificação ao cliente e à ANPD. Registro formal no SGI-10.1-REG-NC-01.
Proteção de dados de processos licitatórios	Informações de propostas, estratégias e valores de licitações são classificadas como RESTRITO (N5) e acessíveis apenas ao gestor da proposta e ao Diretor Comercial.
Uso de IA e ferramentas externas	POL-IA-01 proíbe o uso de dados de clientes em ferramentas de IA não homologadas. A Plataforma Adapta é a única ferramenta autorizada para dados até CONTROLADO (N3). Violação: sanção conforme Seção 15.
Continuidade como obrigação contratual	BCP e DRP documentados e testados anualmente (SGI-BCP-01, SGI-DRP-01). A interrupção dos serviços SOC/MSS pode gerar risco de segurança para os clientes — a continuidade é, portanto, também uma obrigação de integridade contratual.

9.2 Incidente de Segurança como Questão de Integridade

Todo incidente de segurança que envolva dados de clientes tem dupla natureza: técnica (tratado pelo processo SGI-8.6.1-PRC-INC-01) e de integridade (reportado ao CI para avaliação das obrigações contratuais, legais e éticas). A tentativa de ocultar ou minimizar um incidente constitui violação grave do Código de Ética.

⃠ **VEDAÇÃO ABSOLUTA O** sigilo sobre um incidente de segurança que afete dados de clientes, para proteger a reputação da empresa ou evitar consequências comerciais, é tratado como violação de integridade de alta gravidade — equivalente a fraude. O CI tem autoridade para acionar canais externos (CGU, ANPD, clientes) independentemente da posição comercial.

10. PROTEÇÃO DE DADOS PESSOAIS — LGPD E ISO 27701

O tratamento de dados pessoais pela 2R Datatel ocorre em três contextos distintos: (a) dados de colaboradores, (b) dados de clientes dos serviços SOC/MSS (dados pessoais presentes nos ambientes monitorados), e (c) dados de investigações internas de integridade. Cada contexto tem obrigações específicas.

10.1 Princípios Aplicáveis

Princípio LGPD	Aplicação na 2R Datatel
Finalidade (Art. 6º, I)	Dados são coletados e usados exclusivamente para a finalidade informada. Dados obtidos na prestação de serviços SOC/MSS não podem ser utilizados para outros fins sem consentimento.
Necessidade (Art. 6º, III)	Apenas os dados estritamente necessários para a prestação do serviço são coletados e processados.
Transparência (Art. 6º, VI)	Titulares (colaboradores e clientes) são informados sobre o tratamento de seus dados de forma clara e acessível.
Segurança (Art. 6º, VII)	Controles técnicos e organizacionais da ISO 27001 garantem a proteção dos dados pessoais.
Não discriminação (Art. 6º, IX)	Dados pessoais sensíveis (saúde, etnia, religião) não são usados para fins discriminatórios.
Responsabilização (Art. 6º, X)	A 2R Datatel demonstra conformidade com a LGPD por meio do SGI, auditorias e registros — não apenas declara.

10.2 Tratamento de Dados em Investigações de Integridade

As investigações conduzidas pelo CI envolvem, necessariamente, o tratamento de dados pessoais dos envolvidos (investigado, denunciante, testemunhas). Este tratamento segue regras estritas:

- Base legal: legítimo interesse da empresa para proteção de seus direitos e de terceiros (LGPD, Art. 7º, IX) e cumprimento de obrigação legal (Art. 7º, II).
- Minimização: apenas os dados necessários para a investigação são coletados e processados.
- Acesso restrito: dados da investigação acessíveis apenas aos membros do CI e ao DPO. Proibido compartilhar com partes não envolvidas.
- Retenção: dados de investigação retidos pelo prazo prescricional aplicável (mínimo 5 anos). Após, eliminados com registro.
- Anonimização de denúncias: quando a denúncia é anônima, nenhum dado identificador do denunciante é coletado ou armazenado — o sistema não tenta identificar o denunciante.
- Proteção do investigado: os dados do investigado não são divulgados externamente antes de decisão final, salvo obrigação legal ou regulatória.

⚖ **FUNDAMENTO LEGAL LGPD**, Art. 16: dados pessoais devem ser eliminados após o término do tratamento, ressalvadas as hipóteses de retenção legal. O CI mantém registro das bases legais de cada tratamento realizado em investigações de integridade.

11. DIVERSIDADE, EQUIDADE E AMBIENTE DE TRABALHO ÍNTEGRO

Um ambiente de trabalho íntegro é pré-condição para decisões éticas de qualidade. A 2R Datatel trata a promoção da diversidade, a prevenção do assédio e a garantia de igualdade de oportunidades como obrigações de integridade — não como políticas de RH opcionais.

11.1 Compromissos e Controles

Compromisso	Controles e Evidências
Igualdade de oportunidades	Processos seletivos com critérios exclusivamente técnicos e objetivos, documentados. Proibido qualquer critério discriminatório baseado em gênero, raça, etnia, religião, orientação sexual, deficiência ou qualquer outra condição pessoal.
Equidade de gênero — NLLC	Em consonância com a Lei 14.133/2021, as práticas de equidade de gênero da 2R Datatel são documentadas para fins de critério de desempate em licitações. Relatório de equidade disponível para verificação por órgãos públicos contratantes.
Prevenção e resposta a assédio	Canal de denúncias (Seção 12) disponível para relato de assédio moral ou sexual. Investigação obrigatória em até 15 dias. Tolerância zero: comprovado o assédio, desligamento imediato e registro no histórico do colaborador.
Ambiente psicologicamente seguro	Colaboradores podem expressar discordâncias éticas sem medo de retaliação. O Programa de Integridade inclui proteção formal ao denunciante (Seção 12.4). Gestores são avaliados também pela qualidade do clima ético de suas equipes.
ISO 45001 — Saúde e Segurança	O Sistema de Gestão de SSO garante ambiente fisicamente seguro e inclui prevenção de riscos psicossociais (estresse, burnout, assédio) como riscos ocupacionais mapeados e controlados.

12. CANAL DE DENÚNCIAS — ESTRUTURA, FLUXO E PROTEÇÕES

O Canal de Denúncias é o mecanismo pelo qual qualquer pessoa — colaborador, terceiro, cliente ou parceiro — pode reportar condutas em desacordo com este Programa, com o Código de Ética ou com a legislação aplicável, de forma segura, confidencial e sem risco de retaliação.

12.1 Canais Disponíveis

Canal	Descrição	Anonimato
E-mail seguro	canaldedenuncias@2rdatatel.com.br — acesso exclusivo do Responsável pelo Programa (Renato dos Santos). Nenhum outro colaborador tem acesso.	✅ **Possível — não é exigida identificação**
Formulário digital seguro	Formulário hospedado em plataforma de terceiro com criptografia — sem rastreamento de IP. Link disponível na intranet e no site institucional.	✅ **Garantido — tecnicamente anônimo**
Conversa direta (identificada)	Com o Responsável pelo Programa ou com qualquer membro do CI, pessoalmente ou por videoconferência.	❌ **Identificado — maior proteção formal ao denunciante**
Órgãos externos	CGU (Fala.BR), TCU, MP, ANPD — para denúncias que envolvam atos lesivos ao Poder Público ou violações de LGPD.	✅ **Canais independentes — fora da gestão da empresa**

12.2 O que pode ser reportado

- ☐ Suspeita de suborno, corrupção ou vantagem indevida envolvendo colaborador, parceiro ou agente público
- ☐ Uso indevido de ativos, sistemas ou dados da empresa ou de clientes
- ☐ Violação de confidencialidade ou vazamento de dados
- ☐ Conflito de interesses não declarado
- ☐ Assédio moral, sexual ou discriminação
- ☐ Irregularidades em processos licitatórios ou execução de contratos públicos
- ☐ Fraude financeira, contabilidade irregular ou falsificação de registros
- ☐ Violação de políticas internas ou do Código de Ética
- ☐ Qualquer conduta que o denunciante, de boa-fé, acredite ser antiética ou ilegal

12.3 Fluxo de Investigação

	Etapa	Ação	Prazo
1	**Recebimento**	Responsável pelo Programa acusa recebimento (quando identificado o denunciante). Registra no sistema de controle de denúncias com número de protocolo.	Imediato
2	**Triagem inicial**	CI avalia: (a) a denúncia é suficientemente detalhada para investigação? (b) envolve quem? (c) qual o grau de urgência? Classificar como Alta, Média ou Baixa gravidade.	≤ 5 dias úteis
3	**Abertura formal**	CI delibera sobre abertura da investigação. Para denúncias de Alta gravidade: reunião extraordinária em 48h. Para Média/Baixa: pauta da próxima reunião ordinária.	≤ 10 dias úteis
4	**Investigação**	Coleta de evidências, entrevistas (voluntárias), análise de sistemas e registros. O investigado é notificado da investigação em momento oportuno (não antes da preservação de evidências).	≤ 30 dias (prorrogável por 30)
5	**Conclusão e deliberação**	CI emite relatório de investigação com: fatos apurados, conclusão (procedente/improcedente/inconclusivo) e recomendação de providências. Votação formal.	≤ 10 dias após investigação
6	**Sanção ou arquivamento**	Se procedente: aplicar sanção conforme Seção 15 e alçadas da Seção 4.2. Se improcedente: arquivar com registro. Se inconclusivo: monitoramento por 6 meses.	≤ 5 dias após deliberação
7	**Retorno ao denunciante**	Quando identificado: informar o resultado no que não comprometa o sigilo da investigação.	≤ 5 dias após deliberação
8	**Encerramento e registro**	Arquivar toda a documentação com classificação RESTRITO. Retenção mínima: 5 anos.	≤ 5 dias após resolução

12.4 Proteção ao Denunciante

🔑 **PONTO-CHAVE A** 2R Datatel garante proteção formal ao denunciante de boa-fé contra qualquer forma de retaliação: demissão, rebaixamento, exclusão de promoção, assédio ou qualquer outro tratamento prejudicial. A retaliação contra denunciante é tratada como infração disciplinar independente e de gravidade equivalente à infração original.

- Vedado ao investigado e a qualquer colaborador tentar identificar o denunciante anônimo.
- Vedada qualquer mudança na situação funcional do denunciante identificado durante o período de investigação sem aprovação do CI.

- O denunciante que sofrer retaliação pode reportar ao CI, ao DPO ou diretamente ao Diretor Presidente.
- A proteção ao denunciante é permanente — vale mesmo após encerramento da investigação.
- Em denúncias que envolvam crimes ou atos lesivos ao Poder Público: a 2R Datatel não obstruirá o denunciante que optar por acionar órgãos externos (CGU, MP, TCU).

13. TREINAMENTO, COMUNICAÇÃO E CULTURA DE CONFORMIDADE

O treinamento é o mecanismo central de internalização do Programa de Integridade. Não é um evento anual de caixa — é um sistema contínuo de formação, verificação de aprendizado e comunicação reforçada ao longo do ano.

Treinamento	Conteúdo	Público	Frequência
Programa de Integridade — Onboarding	Este Programa completo, Código de Ética, canais de denúncia, vedações e consequências	*Todos os novos colaboradores*	Admissão (antes do 1º dia de trabalho)
Ética e Anticorrupção — Reciclagem	Casos práticos, atualizações normativas, vedações, conflito de interesses, presentes	*Todos os colaboradores*	Anual
Setor Público — Controles Específicos	Lei 14.133/2021, relacionamento com agentes públicos, licitações, vedações	*Time comercial + gestores + Direção*	Anual + antes de processos licitatórios relevantes
ISO 37001 — Due Diligence de Terceiros	Processo de due diligence, listas restritivas, cláusulas antissuborno, registros	*CI + Diretor Comercial + área de compras*	Anual
Segurança da Informação — Uso Responsável	Classificação de dados, uso de IA (POL-IA-01), incidentes, phishing, acesso privilegiado	*Todos os colaboradores*	Semestral + simulações mensais de phishing
LGPD e Privacidade	Tratamento de dados de clientes e colaboradores, bases legais, incidentes, ANPD	*Todos os colaboradores*	Anual
Canal de Denúncias — Sensibilização	Como usar, o que reportar, proteções, anonimato, fluxo de investigação	*Todos os colaboradores*	Semestral
Gestores — Liderança Ética	Tone at the top, detecção precoce de riscos, gestão de conflitos de interesse na equipe	*Gestores e Direção*	Anual

13.1 Verificação e Evidência de Treinamento

- Todo treinamento é realizado via LMS (Learning Management System) com registro de conclusão e nota mínima de 70%.
- Treinamentos de onboarding são pré-requisito para concessão de acesso a sistemas — sem conclusão, sem acesso.
- A taxa de conclusão por treinamento é KPI do Programa (meta ≥ 95%) e reportada ao CI trimestralmente.
- Colaborador que não conclui treinamento obrigatório no prazo: notificação formal e bloqueio de acesso ao LMS até regularização.
- Registros de treinamento são evidências para auditorias do Decreto 11.129/2022 e da ISO 37001 — retidos por 5 anos.

14. MONITORAMENTO, INDICADORES E MELHORIA CONTÍNUA

O Programa de Integridade só é efetivo se monitorado com indicadores objetivos e sujeito ao ciclo de melhoria contínua do SGI (ISO 9001 §10.3 / PDCA). Esta seção define os KPIs do Programa e o calendário de revisão.

14.1 Indicadores do Programa de Integridade

Indicador	Meta	Frequência	Responsável	Alerta se
Taxa de conclusão de treinamentos obrigatórios (%)	**≥ 95%**	Trimestral	*Coord. Qualidade*	*< 90%*
% de colaboradores com DCI assinada e atualizada	**100%**	Semestral	*CI*	*< 100%*
Denúncias recebidas no canal (nº)	**Monitorar**	Trimestral	*Resp. Programa*	*Queda abrupta (indica subnotificação)*
% de denúncias investigadas dentro do prazo	**100%**	Trimestral	*Resp. Programa*	*< 100%*
% de investigações concluídas em ≤ 30 dias	**≥ 90%**	Semestral	*CI*	*< 80%*
Due diligence de terceiros realizadas (%)	**100% dos novos + 100% das revisões anuais**	Anual	*CI*	*< 100%*
Incidentes de SI com implicação de integridade (nº)	**Monitorar (meta: 0)**	Trimestral	*CISO*	*> 0 (avaliar causa raiz)*
Reuniões do Comitê de Integridade realizadas (nº)	**≥ 4/ano (trimestrais)**	Anual	*Resp. Programa*	*< 4*

Tempo médio de encerramento de investigações	**≤ 30 dias**	Semestral	*CI*	*> 45 dias*
Sanções aplicadas no período (nº)	**Monitorar**	Semestral	*CI*	*Ausência prolongada pode indicar subnotificação*
Processos licitatórios com checklist de integridade concluído	**100%**	Por processo	*Dir. Comercial*	*< 100%*
Fornecedores com due diligence atualizada (%)	**100%**	Anual	*CI*	*< 100%*

14.2 Calendário de Revisão e Eventos de Governança

Periodicidade	Evento / Revisão	Responsável
Mensal	Relatório de uso do canal de denúncias + indicadores de SI com implicação de integridade	*Resp. Programa → CI*
Trimestral	Reunião ordinária do CI (pauta mínima Seção 4.2) + relatório de KPIs do Programa	*Resp. Programa*
Semestral	Revisão do mapa de riscos de integridade + due diligence de terceiros recorrentes + relatório de treinamentos	*CI + CISO*
Anual	Revisão completa do Programa de Integridade + aprovação pelo Diretor Presidente + auditoria interna (ISO 37001) + atualização das políticas vinculadas	*CI + Auditoria Interna*
Por evento	Abertura de investigação · Incidente de SI com implicação de integridade · Novo contrato público relevante · Novo parceiro de alto risco · Mudança normativa relevante	*CI (por convocação)*

15. PENALIDADES E RESPONSABILIZAÇÃO

As penalidades por descumprimento do Programa de Integridade são proporcionais à gravidade, à intencionalidade, ao dano causado e à conduta pós-fato (cooperação com a investigação versus obstrução). A tabela abaixo é orientativa — o CI delibera caso a caso.

	Infração	Gravidade	Penalidade Aplicável
G1	Descumprimento de política interna sem impacto externo ou dano (ex.: não concluir treinamento no prazo)	Leve	Notificação formal · Prazo para regularização · Registro no histórico
G2	Uso de ferramenta de IA não autorizada sem inserção de dados sensíveis · Recebimento de brinde acima do limite sem comunicação · Omissão não intencional em DCI	Média	Advertência formal · Treinamento adicional obrigatório · Registro no SGI como NC · Avaliação pelo CI
G3	Conflito de interesses não declarado com impacto em decisão · Compartilhamento não autorizado de informações internas sem dados de clientes · Assédio moral leve · Omissão de denúncia conhecida	Grave	Advertência formal + possível suspensão · Afastamento do processo afetado · Avaliação de demissão · Registro formal no SGI
G4	Vazamento de dados de clientes · Suborno ou tentativa · Irregularidade em processo licitatório · Assédio sexual · Fraude financeira · Obstrução de investigação	Gravíssima	Demissão por justa causa · Notificação ao cliente afetado · Comunicação ao CGU/MP/ANPD (se aplicável) · Ação civil ou criminal por danos
G5	Ato lesivo à Administração Pública (Lei 12.846/2013) · Acesso não autorizado a dados críticos de clientes para benefício próprio · Conluio em licitação	Crítica / Societária	Demissão imediata + todas as medidas de G4 + comunicação obrigatória ao Diretor Presidente + avaliação de denúncia espontânea ao CGU para efeitos de atenuação (art. 7º, §1º, Lei 12.846)

⚠ **ATENÇÃO** A cooperação espontânea com a investigação, a ausência de reincidência e a reparação do dano são atenuantes considerados pelo CI. A reincidência, a obstrução da investigação e o envolvimento de terceiros

(clientes, fornecedores, agentes públicos) são agravantes. Para atos que possam caracterizar crimes, a comunicação às autoridades não é discricionária.

16. DISPOSIÇÕES FINAIS

16.1 Abrangência e Hierarquia

- Este Programa aplica-se a todos os colaboradores, estagiários, prestadores de serviço, parceiros, representantes e qualquer pessoa que atue em nome da 2R Datatel.
- Em caso de conflito entre este Programa e norma interna de menor hierarquia, prevalece o Programa de Integridade. Em caso de conflito com legislação aplicável, prevalece a lei.
- Este Programa não limita, em nenhuma hipótese, os direitos dos colaboradores garantidos pela CLT, pela Constituição Federal e pela legislação trabalhista aplicável.

16.2 Vigência e Revisão

- Vigência: imediata a partir da aprovação pela Direção e assinatura dos responsáveis.
- Revisão: anual obrigatória, a ser realizada pelo CI até 31 de março de cada ano, ou imediatamente após evento relevante (mudança normativa, incidente grave, expansão de negócios).
- O histórico de versões é mantido no SGD (Sistema de Gestão de Documentos) com acesso controlado.

16.3 Canais de Contato

Canal de Denúncias (email)	canaldedenuncias@2rdatatel.com.br
CGU — Fala.BR (canal externo)	https://falabr.cgu.gov.br
ANPD (dados pessoais)	https://www.gov.br/anpd