CONTROL 361 TECNOLOGIA E SERVIÇOS LTDA

POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS

2025 / 2026

CONTROL 361°

Índice

01

PRINCÍPIOS, FUNDAMENTOS E GOVERNANÇA

A Gestão de Riscos da CONTROL 361 será orientada pelos seguintes princípios:

• Legalidade e conformidade regulatória, com aderência integral à legislação vigente, especialmente à Lei nº 13.709/2018 (LGPD);
• Accountability (prestação de contas), assegurando rastreabilidade das decisões;
• Transparência e integridade corporativa;
• Prevenção e mitigação de riscos, priorizando abordagem proativa;
• Segregação de funções, evitando conflitos de interesse;
• Segurança da informação por design e por padrão (privacy by design / by default).

Condutas Obrigatórias

• Registro formal de riscos e incidentes;
• Comunicação tempestiva e documentada;
• Atuação conforme políticas internas e contratos;
• Proteção de dados pessoais e sensíveis.

Vedações Expressas

• Omissão, subnotificação ou atraso na comunicação de incidentes;
• Manipulação de indicadores ou registros;

• Acesso indevido a dados ou sistemas;
• Descumprimento de controles internos.

02

OBJETIVOS E FINALIDADE

A presente Política tem por finalidade instituir e disciplinar o modelo corporativo de gestão de riscos da CONTROL 361 TECNOLOGIA E SERVIÇOS LTDA, com base em práticas reconhecidas de governança e compliance, visando:

1. Estabelecer Diretrizes e Estrutura

• Definir princípios, responsabilidades e processos claros para a gestão de riscos na empresa.
• Padronizar a forma como todos os agentes (colaboradores, fornecedores, terceiros) devem lidar com riscos.
• Estabelecer governança estruturada, com papéis e níveis de responsabilidade, incluindo Alta Administração, Comitê de Riscos, Risk Owners e Auditoria Interna.

2. Identificação e Mitigação de Riscos

• Identificar riscos financeiros, operacionais, tecnológicos, jurídicos,

regulatórios, reputacionais e estratégicos.
• Aplicar critérios objetivos para avaliar probabilidade e impacto, utilizando ferramentas como matriz de risco 5x5.
• Garantir que riscos críticos e altos sejam tratados formalmente, com planos de ação documentados e responsáveis definidos.

3. Garantir Conformidade Legal e Regulamentar

Assegurar aderência às normas legais e regulatórias aplicáveis, incluindo:
• Lei nº 13.709/2018 – LGPD;
• Lei nº 12.846/2013 – Lei Anticorrupção;
• Normas internacionais ISO 31000 (Gestão de Riscos) e ISO 27001 (Segurança da Informação).
• Reforçar obrigações contratuais, responsabilidades de terceiros e registro auditável de todas as ações, decisões e incidentes.

4. Promover Continuidade Operacional

• Orientar a implementação de planos de ação para minimizar impactos de incidentes, falhas de sistemas ou crises corporativas.
• Garantir que riscos críticos sejam escalonados à Alta] Administração e tratados com prioridade.
• Integrar a gestão de riscos ao Business Continuity Planning (BCP), assegurando operação segura e estável.

5. Fomentar Cultura de Riscos e Accountability

• Promover cultura organizacional de prevenção, monitoramento e responsabilidade em todos os níveis da empresa.
• Exigir que todos os agentes tenham ciência formal da política, participem de treinamentos periódicos e cumpram suas responsabilidades.
• Utilizar indicadores de risco (KRIs) e relatórios periódicos para subsidiar decisões estratégicas e operacionais.

6. Proteção da Reputação e Ativos da Empresa

• Minimizar exposição a perdas financeiras, danos à imagem,multas ou ações judiciais.
• Criar evidências de que a empresa age de forma proativa,estruturada e conforme boas práticas de governança corporativa.

03 ABRANGÊNCIA E VINCULAÇÃO CONTRATUAL

A presente Política possui caráter normativo, vinculante e juridicamente defensável, aplicando-se a todos os indivíduos e entidades que, direta ou indiretamente, atuem em nome, interesse ou benefício da CONTROL 361, incluindo:

• Colaboradores, independentemente do regime de contratação (CLT, pessoa jurídica, estagiários e temporários).
• Administradores, diretores e membros da alta gestão.
• Fornecedores, prestadores de serviço e terceiros contratados.
• Parceiros comerciais, tecnológicos e institucionais.

3.1 Obrigatoriedade de Cumprimento

• O cumprimento desta Política é condição obrigatória para manutenção de qualquer vínculo jurídico ou contratual com a CONTROL 361.
• Descumprimento sujeita o agente a medidas disciplinares internas e responsabilização civil, administrativa ou penal, conforme legislação aplicável e cláusulas contratuais.

3.2 Vinculação Contratual Obrigatória

Todos os instrumentos contratuais da CONTROL 361 devem conter cláusula expressa prevendo, no mínimo:

1. **Adesão Integral à Política:** obrigatoriedade de observância integral da Política de Gestão de Riscos e demais normativos internos aplicáveis.
2. **Responsabilidade:** responsabilização objetiva e/ou subjetiva do contratado por danos decorrentes de falhas, omissões ou incidentes.
3. **Comunicação de Incidentes:** obrigação de comunicação imediata (sem atraso injustificado) de qualquer incidente, risco relevante ou potencial violação que possa impactar a CONTROL 361, seus clientes ou dados tratados.

4. **Penalidades Contratuais:** previsão expressa de medidas proporcionais, incluindo, mas não se limitando a:
   ◦ Advertência formal;
   ◦ Multa;
   ◦ Suspensão;
   ◦ Rescisão contratual por justa causa;
   ◦ Responsabilização por perdas e danos.
5. **Auditoria e Fiscalização:** direito da CONTROL 361 de auditar e fiscalizar o cumprimento das obrigações contratuais relacionadas à gestão de riscos e segurança da informação.
6. **Conformidade com LGPD:** obrigação de cumprir integralmente a Lei Geral de Proteção de Dados, incluindo tratamento, segurança, sigilo e resposta a incidentes envolvendo dados pessoais.
7. **Assinatura de Ciência Eletrônica:** a ciência do contratado sobre a política pode ser formalizada por assinatura eletrônica ou digital, com validade jurídica reconhecida pela Lei 14.063/2020.

3.3 Oponibilidade e Evidência de Ciência

A CONTROL 361 deverá assegurar que todos os agentes abrangidos:
• Tenham acesso formal e rastreável à presente Política.
• Declarem ciência e concordância expressa, preferencialmente por meio eletrônico/documental.
• Sejam submetidos, quando aplicável, a treinamentos periódicos de compliance e gestão de riscos, com registro de participação e conteúdo ministrados.

• Todas as evidências de ciência, adesão, treinamentos e auditorias devem ser mantidas de forma auditável e defensável juridicamente, garantindo rastreabilidade em eventuais procedimentos legais, regulatórios ou de fiscalização.

04 ESTRUTURA DE GOVERNANÇA DE RISCOS

A gestão de riscos da CONTROL 361 será estruturada com base no modelo das Três Linhas de Defesa, assegurando segregação de funções, independência e eficácia dos controles internos.

4.1 Alta Administração (Diretoria)

Compete à Alta Administração:
• Definir e formalizar o apetite e a tolerância ao risco da organização;
• Aprovar esta Política e suas revisões periódicas;
• Assegurar a alocação de recursos financeiros, humanos e tecnológicos para a gestão de riscos;
• Deliberar sobre riscos classificados como críticos e sobre eventos de alto impacto;
• Garantir a integração da gestão de riscos à estratégia corporativa.

4.2 Comitê de Riscos e Compliance (quando instituído)

Órgão colegiado de caráter consultivo e/ou deliberativo, com as seguintes atribuições:
• Avaliar e priorizar riscos estratégicos e corporativos;
• Deliberar sobre incidentes relevantes, especialmente aqueles com impacto jurídico, regulatório ou reputacional;
• Monitorar a evolução dos indicadores-chave de risco (KRIs);
• Recomendar melhorias em controles internos e políticas;
• Atuar como instância de apoio à Alta Administração.

4.3 Gestão Executiva (2ª Linha de Defesa)

Compete à Gestão Executiva:
• Implementar esta Política no nível tático e operacional;
• Estruturar e manter atualizada a matriz corporativa de riscos;
• Garantir a implementação e eficácia dos controles internos;
• Consolidar e reportar periodicamente os riscos à Alta Administração;
• Assegurar o cumprimento das obrigações legais e regulatórias aplicáveis.

4.4 Gestores de Área – “Risk Owners” (1ª Linha de Defesa)

São responsáveis diretos pela gestão dos riscos em seus processos:
• Identificar, avaliar e tratar riscos sob sua responsabilidade;
• Implementar e acompanhar planos de ação;
• Monitorar continuamente os indicadores de risco (KRIs);
• Garantir a conformidade dos processos sob sua gestão;
• Reportar tempestivamente incidentes e não conformidades.

4.5 Área de TI e Segurança da Informação (função especializada)

Compete à área:
• Implementar e manter controles técnicos de segurança da informação;
• Gerenciar acessos, vulnerabilidades e incidentes cibernéticos;
• Assegurar a disponibilidade, integridade e confidencialidade dos dados;
• Garantir aderência às normas de segurança e à Lei Geral de Proteção de Dados (LGPD);
• Apoiar investigações e respostas a incidentes.

4.6 Auditoria Interna / Compliance (3ª Linha de Defesa)

Função independente com as seguintes atribuições:
• Avaliar de forma periódica e independente a eficácia da gestão de riscos e dos controles internos;
• Realizar auditorias baseadas em risco;
• Identificar não conformidades e recomendar melhorias;
• Emitir relatórios técnicos independentes à Alta Administração;
• Monitorar a implementação das recomendações.

4.7 Segregação de Funções e Independência

• As funções de execução, controle e auditoria devem permanecer segregadas;
• A área de Auditoria/Compliance deve atuar com independência funcional;
• É vedada a concentração de responsabilidades que comprometa a imparcialidade ou a rastreabilidade dos processos.

05 METODOLOGIA DE GESTÃO DE RISCOS

A gestão de riscos da CONTROL 361 observará processo contínuo, estruturado, rastreável e documentado, composto pelas etapas abaixo:

5.1 Identificação de Riscos

A identificação deverá ocorrer de forma sistemática e periódica, considerando, no mínimo:
• Processos operacionais e fluxos internos;
• Ativos físicos, tecnológicos e informacionais;
• Obrigações legais, regulatórias e normativas;
• Instrumentos contratuais e responsabilidades assumidas;
• Riscos emergentes (tecnológicos, regulatórios e de mercado).
Requisito obrigatório:
Todos os riscos identificados deverão ser formalmente registrados, com descrição clara da causa, evento e possível consequência.

5.2 Análise de Riscos (Modelo Quantitativo e Qualitativo)

A análise considerará critérios padronizados:
• Probabilidade de ocorrência (escala de 1 a 5);
• Impacto potencial (escala de 1 a 5).

Parâmetros mínimos obrigatórios:

Probabilidade:

1 – Raro

2 – Improvável

3 – Possível

4 – Provável

5 – Quase certo

Impacto (avaliado de forma cumulativa):

• Financeiro

• Jurídico/regulatório

• Operacional

• Reputacional

• Proteção de dados (LGPD)

Requisito:

A classificação deverá ser justificada e documentada, vedada atribuição arbitrária.

5.3 Matriz de Risco 5x5

A classificação dos riscos seguirá a matriz a seguir.

Legenda:

B = Baixo | M = Médio | A = Alto | C = Crítico

Regra obrigatória:

Riscos classificados como Alto ou Crítico exigem tratamento formal imediato.

Impacto \ Probabilidade	1	2	3	4	5
5 (Crítico)	M	A	A	C	C
4 (Alto)	M	M	A	A	C
3 (Médio)	B	M	M	A	A
2 (Baixo)	B	B	M	M	A
1 (Muito baixo)	B	B	B	M	M

5.4 Avaliação de Riscos

Consiste na:

• Comparação do nível de risco identificado com o apetite ao risco corporativo;

• Definição de prioridade de tratamento com base em criticidade;

• Formalização da decisão de tratamento ou aceitação.

Vedação:

É proibida a aceitação tácita de riscos sem registro formal e justificativa.

5.5 Tratamento de Riscos

Os riscos deverão ser tratados conforme uma das seguintes estratégias:

• Mitigar: implementação ou reforço de controles internos;

• Evitar: descontinuidade da atividade geradora do risco;

• Transferir: compartilhamento do risco via contratos, seguros ou terceiros;

• Aceitar: mediante justificativa formal, aprovação e registro.

Requisitos obrigatórios para riscos Alto/Crítico:

• Plano de ação documentado;
• Definição de responsável (risk owner);
• Estabelecimento de prazo;
• Definição de indicador de acompanhamento (KRI);
• Registro de evidências de execução.

5.6 Monitoramento e Revisão

O monitoramento deverá ser contínuo e incluir:

• Acompanhamento dos indicadores de risco (KRIs);
• Revisão periódica da matriz de riscos;
• Testes de eficácia dos controles implementados;
• Auditorias internas e/ou externas.

Gatilhos de revisão obrigatória:

• Incidentes relevantes;
• Alterações legais/regulatórias;
• Mudanças operacionais significativas;
• Novos contratos ou serviços.

5.7 Comunicação, Registro e Rastreabilidade

A gestão de riscos deverá garantir:

• Registro obrigatório em sistema, ferramenta corporativa ou planilha controlada;
• Manutenção de histórico completo e auditável;
• Armazenamento de evidências documentais;
• Rastreabilidade das decisões e responsáveis.

Requisito de compliance:

Todos os registros devem ser íntegros, atualizados e disponíveis para auditoria, interna ou externa.

06 CLASSIFICAÇÃO DOS RISCOS

A classificação dos riscos tem por finalidade padronizar sua identificação, análise e tratamento, assegurando consistência metodológica e rastreabilidade.

Todo risco identificado deverá ser classificado, obrigatoriamente, quanto à sua natureza e origem.

6.1 Classificação por Natureza

Os riscos serão categorizados conforme sua essência:

• Operacional: Relacionado a falhas em processos internos, pessoas ou execução de atividades, incluindo erros humanos, falhas de procedimento e interrupções operacionais;
• Tecnológico (Cibersegurança e TI): Associado a falhas em sistemas, infraestrutura tecnológica, indisponibilidade de serviços, vulnerabilidades, ataques cibernéticos e incidentes de segurança da informação;

• Jurídico / Compliance: Decorrente de descumprimento de leis, regulamentos, contratos ou normativos internos, incluindo riscos relacionados à Lei Geral de Proteção de Dados (LGPD) e à Lei Anticorrupção;
• Financeiro: Relacionado a perdas financeiras, fluxo de caixa, inadimplência, erros de precificação, multas e impactos econômicos adversos;
• Reputacional: Vinculado à imagem institucional, percepção pública, confiança de clientes, parceiros e stakeholders;
• Estratégico: Decorrente de decisões estratégicas inadequadas, mudanças de mercado, inovação tecnológica, concorrência ou falhas no planejamento corporativo.

6.2 Classificação por Origem

Os riscos também deverão ser classificados quanto à sua origem:
• Internos
Originados dentro da organização, incluindo processos, pessoas, sistemas e decisões internas;
• Externos
Decorrentes de fatores fora do controle direto da empresa, como:
◦ alterações legislativas ou regulatórias;
◦ condições de mercado;
◦ ações de terceiros;
◦ eventos externos (ex.: ataques cibernéticos, crises econômicas).

6.3 Classificação Multidimensional (Obrigatória)

Um mesmo risco poderá possuir mais de uma classificação,

devendo ser registrado de forma multidimensional, quando aplicável.

Exemplo:
• Vazamento de dados → Tecnológico + Jurídico + Reputacional
Requisito obrigatório:
É vedada a classificação simplificada que não reflita adequadamente a natureza real do risco.

6.4 Padronização e Consistência

• A classificação deverá seguir os critérios desta Política, sendo vedada a criação de categorias não previstas sem aprovação formal;
• A área de Compliance/Auditoria poderá revisar e reclassificar riscos para garantir consistência metodológica;
• Divergências de classificação deverão ser justificadas e registradas.

6.5 Vinculação ao Tratamento de Riscos

A classificação do risco deverá orientar diretamente:
• A definição da estratégia de tratamento;
• A priorização de ações;
• A alocação de responsabilidades;
• O nível de reporte à governança.

07

CRITICIDADE E CRITÉRIOS OBJETIVOS

A criticidade dos riscos será determinada a partir de critérios objetivos e mensuráveis, considerando múltiplas dimensões de impacto.
Todo risco identificado deverá ser classificado com base nas seguintes categorias:

DIMENSÃO	CRITÉRIO OBJETIVO	ESCALA / THRESHOLD
Financeiro	Perda econômica direta ou indireta	Baixo: R$1 – <R$50 mil Médio: R$50 mil – R$500 mil Alto: R$500 mil – R$1 mi Crítico: > R$1 mi
Jurídico / Regulatório	Multas, processos, sanções legais	Baixo: Multa < R$50 mil ou advertência Médio: R$50 mil – R$200 mil ou processo simples Alto: R$200 mil – R$500 mil ou processo complexo Crítico: > R$500 mil ou risco penal
Reputacional	Impacto na imagem ou confiança de stakeholders	Baixo: Incidente local, pouco impacto Médio: Incidente regional Alto: Incidente nacional Crítico: Internacional / mídia negativa intensa
Operacional	Interrupção de processos críticos	Baixo: < 1 dia Médio: 1–3 dias Alto: 3–7 dias Crítico: > 7 dias ou impacto sistêmico
Proteção de dados (LGPD)	Vazamento ou tratamento inadequado de dados pessoais	Baixo: Incidente sem dados sensíveis Médio: Dados de funcionários Alto: Dados de clientes críticos Crítico: Violação massiva ou sensível

Requisitos obrigatórios:

• Todo risco deve ser avaliado em todas as dimensões aplicáveis;

• A criticidade final será determinada pela dimensão de maior impacto;
• Riscos Críticos e Altos exigem plano formal de tratamento e reporte imediato.

Nível 1 - Tolerância Zero:
Descrição: Eventos que comprometam a sobrevivência legal ou reputacional da empresa
Exemplos de Eventos: Vazamento de dados pessoais sensíveis ou em massa- Fraude corporativa- Corrupção- Violação legal grave (multas elevadas, sanções criminais)
Obrigação/Ação: Mitigação ou evitação imediata; registro formal obrigatório

Nível 2 - Baixa Tolerância:
Descrição: Eventos de impacto relevante, mas controlável.
Exemplos de Eventos: Descumprimento contratual relevante- Não conformidade regulatória não crítica - Pequenos incidentes financeiros.
Obrigação/Ação: Monitoramento rigoroso; plano de ação formal.

Nível 3 - Tolerância Moderada:
Descrição: Eventos operacionais ou técnicos com impacto limitado
Exemplos de Eventos: Falhas operacionais não críticas- Interrupções controladas de processos- Pequenas falhas técnicas sem impacto financeiro ou legal significativo
Obrigação/Ação: Registro, monitoramento e melhoria contínua; plano formal opcional

08

PLANO DE TRATAMENTO DE RISCOS

Todo risco classificado como Alto ou Crítico deverá obrigatoriamente possuir plano de tratamento formal, estruturado conforme o seguinte modelo mínimo:

ITEM	DETALHAMENTO
Descrição do risco	Descrever claramente o risco, sua causa, evento e consequência potencial.
Classificação	Probabilidade x impacto, conforme matriz 5x5.
Responsável (Risk Owner)	Nome, cargo e área responsável pela execução.
Plano de ação	Ações para mitigar, evitar, transferir ou aceitar o risco, com recursos necessários.
Prazo de implementação	Datas de início e término, incluindo marcos intermediários.
Indicadores de acompanhamento (KRIs)	Métricas mensuráveis para monitoramento contínuo.
Status	Atualização periódica (mensal/trimestral) do progresso e eficácia.
Escalonamento	Procedimento para comunicar a Alta Administração ou Comitê de Riscos se necessário.
Evidências documentais	Logs, relatórios ou documentos que comprovem execução das ações.

Regras obrigatórias:

• Riscos tratados devem ser monitorados continuamente;
• Mudanças no plano devem ser registradas e justificadas;
• Todo registro deve ser auditável e rastreável;
• Riscos críticos exigem reportes imediatos à Alta Administração e, quando aplicável, ao Comitê de Riscos.

09

INDICADORES DE RISCO (KRIs Key Risk Indicators)

• Os KRIs (Key Risk Indicators) são métricas-chave que permitem monitorar de forma contínua os riscos identificados, fornecendo sinais antecipados de que um risco pode estar se materializando. Eles devem ser:
• Quantitativos e mensuráveis;
• Vinculados à criticidade do risco (Baixo, Médio, Alto, Crítico);
• Objetivos e rastreáveis, com registro formal para auditoria;
• Acionáveis, ou seja, devem permitir a implementação imediata de planos de mitigação ou escalonamento quando os thresholds forem atingidos.
• O uso dos KRIs permite que a empresa:
• Detecte problemas antes que causem impacto significativo;
• Priorize ações de mitigação com base em evidências;
• Forneça relatórios claros para Alta Administração e Comitê de Riscos.

• Garanta conformidade com normas internas, LGPD e regulamentos aplicáveis;
• Abaixo, seguem exemplos de KRIs obrigatórios para monitoramento corporativo:

KRI	TIPO DE RISCO	MÉTRICA	THRESHOLD / ALERTA
Tempo de indisponibilidade de sistemas	Operacional / Tecnológico	Horas/dia	≤2h: Baixo >2h a 6h: Médio >6h a 12h: Alto >12h: Crítico
N° de incidentes de segurança cibernética	Tecnológico / LGPD	Eventos por mês	1–2: Baixo 3–5: Médio >5: Crítico
N° de não conformidades contratuais	Jurídico / Compliance	Incidentes por trimestre	1–2: Baixo 3–4: Médio ≥5: Crítico
Reclamações de clientes	Reputacional / Operacional	Incidentes por trimestre	1–3: Baixo 4–6: Médio >6: Crítico
Incidentes envolvendo dados pessoais	LGPD / Compliance	Eventos registrados	1–2: Médio>2: Alto Violação massiva: Crítico

Regras obrigatórias:
• Todos os KRIs devem ter responsável formal pelo monitoramento;
• Excedentes de thresholds devem gerar alerta automático e escalonamento;
• KRIs devem ser revisados periodicamente para atualização de limites;
• Indicadores devem ser registrados e mantidos auditáveis, com evidências de acompanhamento.

10 GESTÃO DE INCIDENTES

Todos os incidentes, independentemente de sua natureza, devem ser tratados de forma formal, documentada e rastreável, seguindo o fluxo obrigatório:

10.1 Fluxo de Tratamento de Incidentes

1. Identificação imediata
• Qualquer colaborador, terceiro ou sistema que detecte incidente deve registrar imediatamente o evento.

2. Registro formal
• Todos os incidentes devem ser documentados em sistema corporativo ou planilha controlada, incluindo data, hora, responsável pela identificação, descrição detalhada do evento, risco associado e impacto potencial.

3. Comunicação ao gestor responsável
• O gestor da área afetada deve ser informado imediatamente, com cópia para o Risk Owner e Compliance.

4. Escalonamento
• Incidentes classificados como Alto ou Crítico devem ser escalonados à
• Alta Administração e Comitê de Riscos, com registro de todas as ações e decisões.

5. Plano de resposta e mitigação

• Deve incluir ações corretivas, responsáveis, prazos e evidências.

• Para riscos críticos, deve haver ativação do plano de continuidade de negócios (BCP), se aplicável.

6. Relatório final e lições aprendidas

• Consolidar todas as ações, resultados e impactos, com arquivamento auditável.

• Incorporar recomendações para prevenção de reincidência.

10.2 Incidentes envolvendo dados pessoais (LGPD)

Para incidentes que envolvam dados pessoais, devem ser observadas obrigatoriamente:

• Comunicação imediata ao Encarregado pelo Tratamento de Dados (DPO);

• Avaliação formal de Risco e Impacto à Proteção de Dados (DPIA);

• Notificação à Autoridade Nacional de Proteção de Dados (ANPD), quando aplicável;

• Registro completo de todas as ações tomadas, evidências e comunicações;

• Escalonamento interno conforme criticidade e apetite ao risco.

Regra obrigatória:

A não observância do fluxo de incidentes configura descumprimento desta política, sujeitando o responsável às penalidades internas e contratuais.

11 BASE LEGAL E REFERENCIAL NORMATIVO

A presente Política fundamenta-se em normas legais, regulatórias e boas práticas de governança corporativa:

• Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD);

• Lei nº 12.846/2013 – Lei Anticorrupção;

• ISO 31000 – Gestão de Riscos;

• ISO 27001 – Sistema de Gestão de Segurança da Informação;

• Boas práticas de governança corporativa, auditoria interna e compliance;

• Normativos internos da CONTROL 361, incluindo contratos, manuais e procedimentos operacionais.

Observações:

• Todos os colaboradores, fornecedores e terceiros vinculados devem atuar estritamente em conformidade com estas normas;

• Alterações legislativas ou regulatórias devem ser incorporadas imediatamente, mediante revisão formal da política;

12 AUDITORIA, CONTROLE E SANÇÕES

12.1 Auditoria e Controle

• Serão realizadas auditorias internas e externas periódicas para verificar o cumprimento desta Política e das normas correlatas;
• Todos os registros de risco, planos de ação, KRIs e incidentes deverão ser documentados e auditáveis;
• Não conformidades identificadas deverão ser registradas formalmente, com análise de causa, plano corretivo e responsáveis designados;
• O Compliance e a Auditoria Interna têm autoridade para revisar, classificar e reclassificar riscos, bem como verificar execução de planos de mitigação.

12.2 Medidas Disciplinares e Responsabilização

O descumprimento desta Política sujeitará o infrator às seguintes medidas, conforme gravidade do caso:
• Advertência formal;
• Suspensão temporária das funções;
• Rescisão contratual por justa causa, nos casos aplicáveis;
• Responsabilização civil, administrativa ou penal, de acordo com a legislação vigente e contrato aplicável;
• Registro de todas as ações disciplinares para rastreabilidade e auditoria.

Regra obrigatória:
A aplicação de sanções deve ser documentada, proporcional e transparente, assegurando o devido processo interno.

13 VIGÊNCIA, REVISÃO E EFICÁCIA

• Esta Política entra em vigência imediata após aprovação pela Diretoria;

• Revisão da Política:

- Ordinária: a cada 2 (dois) anos;
- Extraordinária: sempre que houver alterações legais, regulatórias, tecnológicas ou estratégicas significativas;

• A Política é obrigatória e vinculante para todos os colaboradores, fornecedores, parceiros e terceiros vinculados à CONTROL 361;
• Não cumprimento desta Política será considerado descumprimento de norma interna e poderá gerar as sanções previstas no item 13;
• Todas as revisões devem ser registradas formalmente, com versão, data e aprovação da Diretoria, garantindo rastreabilidade e validade jurídica.

14

TERMO DE APROVAÇÃO

Documento aprovado pela Diretoria da
CONTROL 361 TECNOLOGIA E SERVIÇOS LTDA, com força normativa interna e vinculante.

CONTROL 361°

2025/2026