POLÍTICA DE CONTRATAÇÃO DE TERCEIROS

1. INTRODUÇÃO E ESCOPO

Esta Política estabelece o framework de segurança e integridade exigido de todos os fornecedores e subcontratados (doravante denominados coletivamente como "Terceiros") do Escritório Malta Advogados.

Este documento aplica-se a todos os Terceiros e visa garantir a proteção de ativos de informação, incluindo dados pessoais de clientes, informações legais e dados organizacionais.

Além disso, é imperativo que os parceiros demonstrem compromisso com os padrões éticos estabelecidos e possuam governança interna para prevenir práticas comerciais antiéticas, corrupção, fraude e violações de direitos humanos.

Os Terceiros devem cumprir integralmente leis anticorrupção nacionais e internacionais, regimes de sanções e obrigações da Lei Geral de Proteção de Dados (LGPD).

Destaca-se que o Escritório não terceiriza sua atividade-fim, limitando a contratação a serviços de suporte, logística e necessidades operacionais subsidiárias.

Por fim, reforça-se que a contratação de Terceiros é condicionada à aprovação em processo de *due diligence* e à classificação de risco conforme a criticidade do serviço e sensibilidade dos dados.

2. OBJETIVO DA POLÍTICA

Esta Política tem por objetivo estabelecer diretrizes normativas para o ciclo completo das relações com Terceiros, compreendendo as etapas de seleção, diligência, contratação e monitoramento.

Busca-se, por meio deste instrumento, mitigar riscos de natureza operacional, regulatória, cibernética, financeira e reputacional, assegurando que a atuação de Terceiros não comprometa a integridade, a segurança e a continuidade das atividades do Escritório.

Adicionalmente, a Política visa garantir a plena conformidade com a legislação aplicável e com padrões normativos nacionais e internacionais, incluindo a Lei Anticorrupção Brasileira, a Lei Geral de Proteção de Dados (LGPD), bem como o Foreign Corrupt Practices Act (FCPA) e o UK Bribery Act.

Por fim, estabelece-se como diretriz a exigência de que terceiros classificados como críticos adotem controles adequados de segurança, governança e continuidade, de modo a resguardar os ativos de informação e a resiliência operacional do Escritório.

3. ABRANGÊNCIA E RESPONSABILIDADE

As diretrizes estabelecidas nesta Política são de observância obrigatória para todos os Terceiros e seus subcontratados que, direta ou indiretamente, processem dados organizacionais ou de clientes (“quartas partes”). O cumprimento integral desta norma constitui condição indispensável para a manutenção de qualquer vínculo contratual ou institucional com o Escritório, devendo ser observado de forma contínua ao longo de toda a relação.

Cabe ao Terceiro contratado assegurar que sua cadeia de subcontratação adote padrões de segurança, integridade e conformidade equivalentes aos exigidos pelo Escritório.

Adicionalmente, reforça-se a necessidade de se promover uma cultura de vigilância e integridade, sendo responsabilidade de todo Terceiro reportar, de forma imediata, quaisquer sinais de alerta (red flags) ou suspeitas de violação.

4. ARCABOUÇO REGULATÓRIO

A presente Política fundamenta-se em normativos nacionais, internacionais e internos que orientam a atuação do Escritório em matéria de integridade, conformidade e gestão de riscos.

No âmbito nacional, destaca-se a Lei Geral de Proteção de Dados (LGPD) e a Lei Anticorrupção e, no plano internacional, a Política observa os parâmetros estabelecidos pelo *Foreign Corrupt Practices Act* (FCPA), pelo *UK Bribery Act*, e pela Convenção das Nações Unidas contra a Corrupção, incorporando padrões globais de prevenção à corrupção e promoção da ética empresarial.

Já no âmbito interno, integram este arcabouço o Código de Ética e Conduta e a Política de Privacidade do Escritório.

5. DIRETRIZES DE HOMOLOGAÇÃO E CLASSIFICAÇÃO

5.1. Classificação de Risco e Inventário

O Escritório mantém um inventário centralizado de ativos SaaS e IaaS, os quais são classificados conforme o nível de risco que representam para as operações, a segurança da informação e a continuidade dos serviços. Este registro é automatizado via MDM e revisado a cada 12 meses.

São considerados de risco crítico os Terceiros responsáveis por infraestrutura essencial, incluindo serviços de computação em nuvem, gestão de identidade e acesso (IAM), gerenciamento de dispositivos móveis (MDM) e soluções de backup, a exemplo de Microsoft, Acronis e Wenz Tecnologia.

Enquadram-se como de alto risco os fornecedores relacionados a sistemas de gestão jurídica, ferramentas de análise de documentos e soluções de segurança de endpoint, como Thomson Reuters, Enter OS, Doc9 e Bitdefender.

Por sua vez, classificam-se como de médio risco os Terceiros responsáveis pelo fornecimento de hardware de rede local e pela gestão de perímetro, como Ubiquiti.

5.2. *Due Diligence* Pré-Contratual

O processo de *due diligence* pré-contratual inicia-se com a coleta estruturada de informações, mediante o envio dos documentos necessários. Na sequência, são realizadas verificações técnicas, compreendendo a avaliação da capacidade operacional, da expertise e da qualificação do fornecedor, bem como a consulta a cadastros governamentais de restrição, incluindo CEIS, CNEP, CEPIM e CADIRREG.

Adicionalmente, procede-se à análise reputacional, por meio de pesquisas em fontes abertas e veículos de mídia, com o objetivo de identificar eventual envolvimento em práticas ilícitas, riscos de integridade ou situações que possam impactar negativamente a reputação do Escritório.

6. MONITORAMENTO CONTÍNUO E VERIFICAÇÃO TÉCNICA

O monitoramento de Terceiros é realizado de forma contínua, com o objetivo de assegurar a manutenção dos níveis de segurança, conformidade e aderência contratual.

As atividades de verificação técnica incluem a revisão periódica de logs de acesso no Microsoft Entra ID, a validação de criptografia em dispositivos gerenciados por meio do Microsoft Intune, incluindo a verificação de chaves BitLocker, e a análise das configurações de compartilhamento no SharePoint Online, de modo a mitigar riscos de exposição indevida de informações.

Adicionalmente, são coletados, em periodicidade anual, relatórios de auditoria independente para Terceiros classificados como críticos, com o objetivo de confirmar a vigência e a abrangência de suas certificações de segurança e conformidade.

7. GESTÃO DE QUARTA PARTE

O Malta Advogados gerencia o risco de quarta parte como componente integrante do processo de onboarding e das revisões periódicas da gestão de riscos de Terceiros, com o objetivo de assegurar visibilidade, controle e alinhamento da cadeia de subcontratação aos padrões exigidos pelo Escritório.

Adicionalmente, exige-se transparência integral quanto à cadeia de sub-processamento de dados, especialmente no caso de provedores de tecnologia, devendo ser plenamente divulgados os subcontratados envolvidos na prestação do serviço, incluindo infraestruturas e plataformas utilizadas.

No caso específico de soluções baseadas em inteligência artificial, é obrigatória a previsão contratual de compromisso de "Zero Data Retention", assegurando que os dados eventualmente processados não sejam armazenados nem utilizados para fins de treinamento de modelos ou qualquer outra finalidade diversa da execução do serviço contratado.

8. CLÁUSULAS CONTRATUAIS RECOMENDADAS

Os contratos celebrados com Terceiros que envolvam o processamento de dados pessoais ou o acesso a informações organizacionais confidenciais devem conter cláusulas específicas destinadas à mitigação de riscos legais, regulatórios e reputacionais.

As partes devem comprometer-se a observar integralmente a legislação anticorrupção aplicável, incluindo a Lei nº 12.846/2013 e normas internacionais correlatas, devendo o Terceiro manter registros contábeis fidedignos, adotar controles internos eficazes e reportar de forma detalhada os serviços prestados. A violação dessas obrigações deve ensejar a possibilidade de rescisão imediata por justa causa, sem prejuízo da apuração de perdas e danos.

No âmbito da proteção de dados pessoais, o Terceiro deve atuar estritamente conforme as instruções documentadas do Escritório, na qualidade de operador, adotando medidas técnicas e administrativas adequadas à proteção das informações, incluindo controles de acesso, criptografia e governança de dados. Eventuais incidentes de segurança devem ser comunicados sem demora indevida, em conformidade com os prazos legais e contratuais aplicáveis.

A obrigação de confidencialidade deve abranger todas as informações técnicas, jurídicas, financeiras e comerciais compartilhadas, incluindo dados protegidos por sigilo profissional, devendo subsistir mesmo após o encerramento da relação contratual.

Ao término do contrato, o Terceiro deverá proceder à devolução ou exclusão segura de todos os dados sob sua responsabilidade, mediante confirmação formal por escrito.

No que se refere à gestão de Quarta Parte, deve-se assegurar que qualquer subcontratação pelos fornecedores do Escritório dependa de sua autorização prévia e que os contratos firmados reflitam, no mínimo, os mesmos padrões de segurança, privacidade e integridade exigidos pelo Malta Advogados.

Por fim, o Escritório se reserva o direito de realizar auditorias periódicas ou sob demanda, podendo exigir, no caso de Terceiros críticos, a apresentação de relatórios de auditoria independente, como certificações reconhecidas de mercado.

ANEXO I – PROCEDIMENTO DE BUSCA E BACKGROUND CHECK

A diligência prévia de Terceiros constitui etapa obrigatória do processo de homologação de fornecedores e poderá ser conduzida internamente ou com o apoio de consultorias especializadas, mediante a utilização de fontes públicas, bases oficiais e ferramentas de monitoramento de risco.

O objetivo do procedimento é identificar riscos de integridade, reputacionais, legais, financeiros e operacionais associados ao Terceiro, seus sócios, administradores e beneficiários finais, de modo a subsidiar a tomada de decisão quanto à sua contratação.

A análise deverá contemplar, no mínimo, as seguintes etapas:

1. Inicialmente, deverá ser realizada pesquisa reputacional em fontes abertas e veículos de mídia, incluindo buscas estruturadas com o nome da pessoa jurídica, seus sócios e administradores, associados a termos indicativos de irregularidades, tais como corrupção, fraude, improbidade administrativa, lavagem de dinheiro, suborno, sanções, investigações ou condenações.

2. Deverão ser realizadas consultas a listas restritivas e bases oficiais, incluindo, mas não se limitando, ao Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), ao Cadastro Nacional de Empresas Punidas (CNEP), ao Cadastro Integrado de Condenações por Ilícitos Administrativos (CADIRREG), bem como ao Cadastro Nacional de Condenações por Improbidade Administrativa do Conselho Nacional de Justiça.

3. Deverá, ainda, ser verificada a eventual existência de acordos de leniência, termos de ajustamento de conduta ou processos de colaboração envolvendo o Terceiro, como indicativo relevante de risco de integridade.

Sempre que aplicável, deverão ser analisados documentos societários, registros cadastrais, certidões de regularidade fiscal e

trabalhista, bem como demonstrações financeiras recentes, com o objetivo de avaliar a regularidade jurídica e a capacidade econômico-financeira do Terceiro.