



COMPLIANCE

POLÍTICA DE DILIGÊNCIAS

CÓDIGO: SEC.CMP.P06

REVISÃO: 00

DATA: 26/09/2023

SECURITY SERVIÇOS AUXILIARES DE TRANSPORTE AÉREO LTDA

POLÍTICA DE DILIGÊNCIAS *PROGRAMA DE COMPLIANCE*

ELABORAÇÃO	VERIFICAÇÃO	VERIFICAÇÃO	APROVAÇÃO
Santiago Compliance Compliance Officer Externo	Rafael Melão Jurídico	Nilson Wanderlei CFO	João Pedro Neves CEO

INTRODUÇÃO

A SECURITY SATA possui um programa de integridade robusto e completo que contempla todos os pilares do compliance e da legislação brasileira. Visando esclarecer e simplificar a forma de entendimento do funcionamento das diligências duplas (Due Diligence) a presente política foi criada.

Esta política é um complemento ao Código de Conduta ética da SECURITY SATA.

OBJETIVO

O objetivo desta Política de Due Diligence é estabelecer as regras e diretrizes para a realização de diligências prévias a contratação de novos parceiros comerciais.

ABRANGÊNCIA

Esta política deve ser observada por todos os colaboradores da SECURITY SATA, principalmente nos contratos acima de R\$ 10.000,00 (dez mil reais) mensais.

DILIGÊNCIAS

Toda relação com terceiros envolvendo a **SECURITY SATA**, acima de R\$ 10.000,00 (dez mil reais) mensais, deve preceder de detalhada pesquisa a respeito do histórico da outra parte, abrangendo práticas comerciais, estrutura administrativa e societária, eventual envolvimento em práticas comerciais obscuras ou ilegais, transparência em suas transações, relacionamentos com autoridades públicas ou pessoas politicamente expostas, adoção aos princípios éticos e morais valorizados por esta empresa, entre outros.

Em razão do princípio da dupla diligência, os setores de contratação e a Área de Compliance devem estar alinhados, submetendo aqueles que transacionem com a empresa às diligências prévias às contratações, com o intuito de averiguar se a relação acarretará em riscos de integridade.

A situação de risco pode ser identificada quando conclui-se que a outra parte não pratica conduta ética, portanto, destoando dos valores de integridade adotados e praticados pela empresa. Nesse caso, a Área de Compliance é responsável pela construção dos procedimentos necessários a cada avaliação, devendo ser executado pelos demais setores responsáveis.

As diligências também observarão a existência ou não de conflito de interesses.

A reprovação na avaliação desses riscos deve ser decisiva para a continuidade da contratação. Podendo a Área de Compliance, no entanto, mensurar o risco e ofertar (aos casos com

menor potencial ofensivo) a oportunidade da outra parte se adequar e também formalizar suas políticas de integridade. A situação é excepcional, devendo ser aplicada apenas aos casos mais brandos, conforme avaliação do profissional de Compliance (responsável por quantificar um tempo razoável para ajuste e conferir se a outra parte realmente adequou-se).

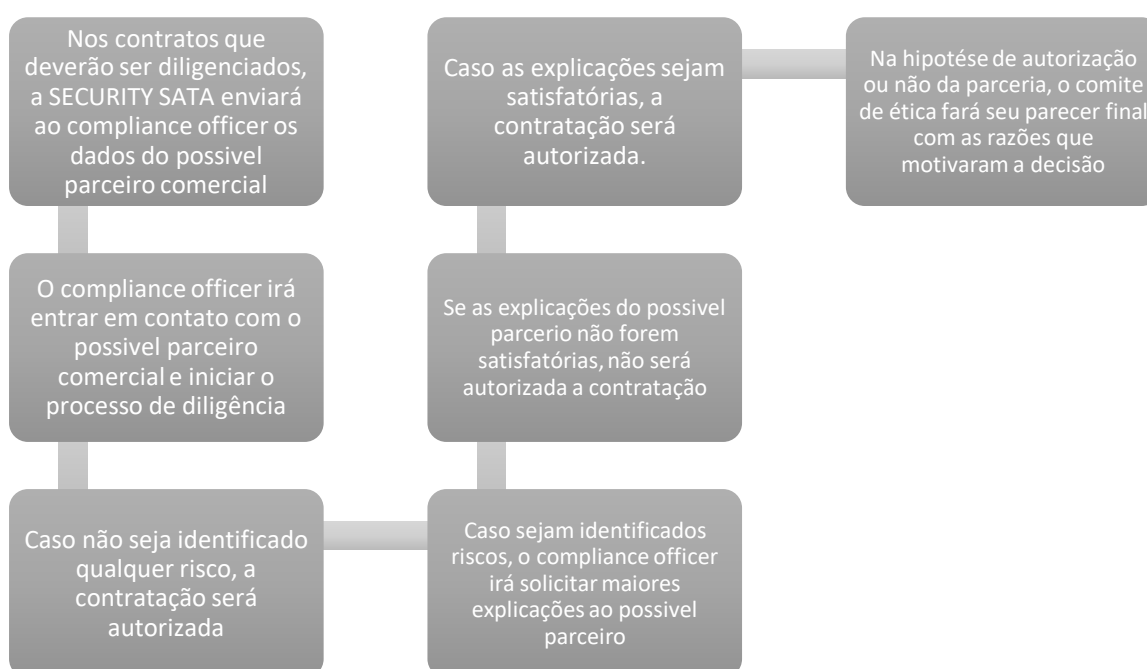
A **SECURITY SATA** entende a hipótese válida, vez que promove a pulverização da cultura ética no mercado. Todavia, tem ciência que deve assim proceder apenas em casos com menor intensidade de risco de integridade. Aos casos que se identifique maior risco, a empresa deve classificar como “*red flag*”, significando situação em que a tratativa será finalizada.

A rescisão ou não efetivação de contratos com empresas que praticam condutas ilegais ou antiéticas, especialmente de fraude ou corrupção, ou ainda que não demonstrem respeito a integridade, é imperioso, por isso, os contratos da **SECURITY SATA** deverão conter cláusulas específicas nesse sentido.

Obviamente as empresas que detenham programas de Compliance são melhores avaliadas. Para avaliação da Área de Compliance, são analisados critérios claros, transparentes, imparciais e compatíveis com as características dos agentes e do negócio. Devendo o posicionamento do Compliance Officer ser exarado de forma técnica e objetiva em formato de parecer.

PROCEDIMENTO DE REALIZAÇÃO DAS DILIGÊNCIAS

As diligências prévias serão feitas da seguinte forma:



I. CANAL DE DENÚNCIAS E COMUNICAÇÃO

A **SECURITY SATA** dispõe de um Canal de Denúncias idôneo, pelo qual qualquer pessoa pode registrar uma ocorrência de eventual conduta antiética, de forma anônima ou identificada, sendo totalmente garantido não haver qualquer tipo de retaliação ao denunciante.

A utilização do Canal deve ser sempre incentivada pela empresa, através de diferentes métodos, tanto aos seus colaboradores, quanto a terceiros.

Qualquer um que suspeitar ou descobrir conduta ilegal ou antiética, deve imediatamente reportar-se à Área de Compliance, através do canal de denúncias: <https://santiagocompliance.com.br/integridade/security-servicos-auxiliares-de-transporte-aereo-lda>, pelo e-mail integridade@santiagoac.adv.br, ou pelo telefone: **(61) 3201 – 9266**.

É fundamental que a utilização do canal de denúncias seja feita de forma adequada e com boa-fé, não sendo admitidas distorções com o objetivo de satisfazer interesses próprios, de terceiros ou prejudicar a imagem de outros. Sendo certa a submissão às consequências disciplinares e legais cabíveis àquele que usar de má-fé.

O denunciante de boa-fé não sofrerá, em hipótese alguma, qualquer tipo de retaliação pela empresa.

O teor das denúncias será tratado pela Área de Compliance de forma confidencial, obedecendo sempre os princípios da presunção da inocência, impessoalidade, imparcialidade, sigilo e respeito pelo Compliance. Ao final do procedimento de investigação, o resultado será divulgado apenas para o comitê de ética, que, em conjunto, decidirá o que deverá ser feito.

Frisa-se que, durante a apuração, sendo grave a acusação e se confirmada, os funcionários e terceiros podem sofrer as medidas disciplinares abaixo.

II. MEDIDAS DISCIPLINARES

A violação ao presente Código, bem como às políticas internas da **SECURITY SATA** ou à legislação brasileira em vigor, sujeitará os responsáveis à medidas disciplinares, podendo ser:

- III. **Advertência;**
- IV. **Suspensão;**
- V. **Dispensa por justa causa ao empregado;**
- VI. **Rescisão contratual;**
- VII. **Multas;**
- VIII. **Comunicação às autoridades competentes;**

O rol acima não é taxativo, apenas exemplificativo e em todos os procedimentos, será observada a legislação aplicável, sendo garantido ao colaborador ou a terceiros o direito constitucional do contraditório e da ampla defesa.

Independente das consequências disciplinares, e por meio de decisão conjunta, as denúncias poderão, após apuradas, ser objeto de representações perante o Ministério Público e órgãos competentes.

IX. CONSIDERAÇÕES FINAIS

O Código de Conduta Ética é o documento principal e faz parte do projeto de Compliance da **SECURITY SATA**, esta política é um complemento ao CCE e será aplicada da mesma forma e com o mesmo alcance que o código de ética.

O documento deve, portanto, ser conhecido por todos que compõem a **SECURITY SATA**, sendo aplicado e rigidamente cobrado a todos, independentemente de grau ou hierarquia, devendo também ter seu conteúdo informado a quaisquer terceiros que tenham, ou pretendam ter, negócios com a empresa, para que saibam os valores e princípios adotados, os quais também devem compartilhar.

O programa de Compliance da SECURITY SATA é contínuo e, por isso, não deve parar de crescer. Sendo papel de cada um buscar essa evolução, que significará ganho para TODOS.

A intenção com a implementação deste programa de Compliance é criar uma cultura ÉTICA entre todos os nossos colaboradores, para então nos tornarmos uma empresa cada vez mais consciente e de caráter ilibado.

Assinatura eletrônica

João Pedro de Noronha Neves
CEO



Datas e horários baseados no fuso horário (GMT -3:00) em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinatura gerado em 15/11/2023 às 10:30:11 (GMT -3:00)

8. Política de Due Diligence (14)

ID única do documento: #b53e5ecf-e1b3-428b-bccf-c3a2c20ecdd3

Hash do documento original (SHA256): a5736c78cde512d187960bbbac248df36aea889b2419e24a6fbd14c2b537c547

Este Log é exclusivo ao documento número #b53e5ecf-e1b3-428b-bccf-c3a2c20ecdd3 e deve ser considerado parte do mesmo, com os efeitos prescritos nos Termos de Uso.

Assinaturas (4)

- ✓ **JOÃO PEDRO DE NORONHA NEVES (Participante)**
Assinou em 16/11/2023 às 14:19:53 (GMT -3:00)
- ✓ **Nilson Lacerda Wanderlei (Participante)**
Assinou em 15/11/2023 às 13:46:57 (GMT -3:00)
- ✓ **Raphael Montagnon (Participante)**
Assinou em 16/11/2023 às 09:40:59 (GMT -3:00)
- ✓ **Rafael Silva Melão (Participante)**
Assinou em 16/11/2023 às 09:38:21 (GMT -3:00)

Histórico completo

Data e hora	Evento
15/11/2023 às 10:30:11 (GMT -3:00)	Millena Rabelo solicitou as assinaturas.
15/11/2023 às 13:46:57 (GMT -3:00)	Nilson Lacerda Wanderlei (Autenticação: e-mail nilson.wanderlei@eps.eng.br; IP: 177.235.151.92) assinou. Autenticidade deste documento poderá ser verificada em https://verificador.contraktor.com.br . Assinatura com validade jurídica conforme MP 2.200-2/01, Art. 10o, §2.

Data e hora

16/11/2023 às 09:38:21
(GMT -3:00)

Evento

Rafael Silva Melão (Autenticação: e-mail rafael@meloadvogados.com.br; IP: 164.163.2.2) assinou. Autenticidade deste documento poderá ser verificada em <https://verificador.contraktor.com.br>. Assinatura com validade jurídica conforme MP 2.200-2/01, Art. 10o, §2.

16/11/2023 às 09:40:59
(GMT -3:00)

Raphael Montagnon (Autenticação: e-mail raphael@santiagoac.adv.br; IP: 177.17.188.96) assinou. Autenticidade deste documento poderá ser verificada em <https://verificador.contraktor.com.br>. Assinatura com validade jurídica conforme MP 2.200-2/01, Art. 10o, §2.

16/11/2023 às 14:19:53
(GMT -3:00)

JOÃO PEDRO DE NORONHA NEVES (Autenticação: e-mail joao.neves@securitysata.com.br; IP: 164.163.2.2) assinou. Autenticidade deste documento poderá ser verificada em <https://verificador.contraktor.com.br>. Assinatura com validade jurídica conforme MP 2.200-2/01, Art. 10o, §2.