Programa Global de Compliance relativo a Responsabilidade Criminal Corporativa

telematica
SISTEMAS INTELIGENTES

www.telematica.com.br

Índice

INTRODUÇÃO

A TELEMÁTICA SISTEMAS INTELIGENTES LTDA., ("**TSI**") é uma empresa limitada, no mercado há mais de 40 (quarenta) anos que atua no mercado da tecnologia de captura de dados para ponto eletrônico.

São aproximadamente 60.000 terminais e controladores instalados em cerca de 8.000 clientes, participando diariamente da vida de mais de 2.500.000 de pessoas. Tudo graças ao esforço e a capacidade de nossos colaboradores e parceiros. Atendendo a todo o território nacional em caráter consultivo, comercial e técnico, através de revendedores e centros autorizados de assistência técnica ou diretamente em conjunto com esses, estamos sempre próximos dos nossos clientes.

A Telemática é totalmente comprometida com a política da qualidade, certificada na norma ISO 9001. Atuando nos segmentos de controle de ponto e acesso, segurança eletrônica integrada, automação de freqüência, bilhetagem eletrônica especialmente em aplicações metro-ferroviárias e estádios de futebol e Automação Predial, a Telemática tem a certeza de que sempre poderá agregar valores e otimizar recursos nos negócios de seus clientes.

Nesse contexto, a integridade é compreendida como um valor fundamental para a condução dos negócios. Isso exige que todos os funcionários do Grupo operem com lealdade, correção, transparência e em estrito cumprimento das leis e regulamentos nacionais e estrangeiros, normas e diretrizes internacionais.

O "**Programa Global de Compliance TSIPG"** foi concebido como uma ferramenta para reforçar o compromisso da TSI com os mais elevados padrões éticos, legais e profissionais para o aprimoramento e preservação da reputação do Grupo. Para

este fim, o programa estabelece uma série de medidas preventivas relativas à responsabilidade criminal corporativa.

Nos últimos anos, o número de países que estabeleceram um regime de responsabilidade corporativa criminal ou *quasi*-criminal – permitindo que tribunais punam pessoas jurídicas por condutas criminais por parte de seus representantes, empregados ou terceiros atuando em seu nome – vem aumentando.

Em algumas jurisdições, as leis e regulamentos aplicáveis estimulam as empresas a adotarem estruturas de governança corporativa e sistemas de prevenção de riscos para envidar esforços a fim de evitar que administradores, executivos, empregados e consultores e contratados externos cometam crimes, prevendo também uma isenção ou mitigação das penalidades aplicáveis na hipótese de adoção de medidas preventivas adequadas.

O TSIPG, inspirado pelos mais importantes regulamentos internacionais, visa definir **normas** gerais de conduta aplicáveis a empregados, diretores e todos os demais membros dos órgãos de administração e controle ("**Destinatários Corporativos**"), bem como consultores ou outros contratados e, de forma geral, terceiros ("**Terceiros**" ou "**Outros Destinatários**") (doravante os Destinatários Corporativos e os Outros Destinatários serão designados em conjunto "**Destinatários**").

Nos casos em que leis e regulamentos locais contenham exigências específicas diferentes das disposições do TSIPG, tais exigências deverão prevalecer.

1. MISSÃO

O TSIPG representa uma oportunidade de reforçar a prevenção proativa de responsabilidade criminal corporativa através do aprimoramento do sistema de governança e controles internos, e é concebido para dar suporte a condutas apropriadas e legais em todo o Grupo.

O TSIPG identifica os principais padrões de conduta esperados detodos os Destinatários Corporativos e – quando especificado – dosOutros Destinatários no intuito de:

(i) Fornecer aos destinatários corporativos e terceiros um conjunto padrão de regras destinadas a prevenir uma responsabilidade criminal corporativa no respectivo país;

(ii) integrar qualquer programa local de compliance de acordo com qualquer lei sobre responsabilidade criminal corporativa aplicável.

As regras contidas no EGCP são integradas por:

i. as disposições estabelecidas no Código de Ética, que representa os princípios éticos do Grupo os quais todos os Destinatários são obrigados a cumprir;

ii. as disposições estabelecidas no Plano de Tolerância Zero com a Corrupção adotado por todo o Grupo TSI;

iii. as disposições de governança corporativa adotadas pelos destinatários e terceiros, refletindo as leis aplicáveis e melhores práticas internacionais;

iv. as disposições estabelecidas em qualquer programa local de compliance adotado por um terceiro a fim de cumprir suas próprias leis locais relativas a responsabilidade criminal corporativa e em quaisquer diretrizes, políticas ou documentos organizacionais internos correlatos.

2. ESTRUTURA

O EGCP identifica:

a) as modalidades de sua adoção pelos destinatários e terceiros e os respectivos processos de atualização;

b) sua disseminação para os Destinatários e atividades de treinamento;

c) o sistema disciplinar aplicável em caso de violação de qualquer disposição contida no mesmo;

d) normas gerais de controle;

e) áreas de atividade a serem monitoradas em relação a certos tipos de condutas ilícitas (as "**Áreas a Serem Monitoradas**" ou "**ASM**") – conforme elencadas na Seção 7 – que são geralmente consideradas crimes e podem potencialmente ser cometidas por um terceiro e a prevenção das quais a TSI considera ser uma prioridade para a condução de seus negócios com honestidade e integridade (os "**Crimes**");

f) principais padrões de conduta ligados às Áreas a Serem Monitoradas.

3. ADOÇÃO, IMPLEMENTAÇÃO, RESPONSABILIDADE E ADITIVOS SUBSEQUENTES

O EGCP foi aprovado pelo Conselho de Administração da TSI e deverá ser aprovado pelo conselho de administração.

O Conselho de Administração ou outro órgão de administração em observância de sua própria autonomia e independência:

(i) adota as medidas mais adequadas para implementação e monitoramento do EGCP, levando em consideração o tamanho, a complexidade das atividades desenvolvidas, o sistema de controles internos e o perfil de risco específico da respectiva TSI e seu quadro regulatório;
(ii) é responsável pela correta implementação das Áreas a serem Monitoradas e dos Principais Padrões de Conduta, conforme estabelecido na seção 9.2 do EGCP, bem como dos controles estabelecidos pelo Programa Global de Compliance da TSI.

O EGCP deverá ser aplicado de acordo com a legislação aplicável, tipo de negócios desenvolvidos, bem como características específicas de sua estrutura organizacional.

Outras alterações substanciais e aditamentos ao EGCP serão confiadas ao Conselho de Administração da TSI e serão posteriormente aprovadas pelo conselho de administração ou por outro órgão de administração.

4. DISSEMINAÇÃO DO EGCP E ATIVIDADES DE TREINAMENTO

O EGCP estará disponível e o download poderá ser efetuado através do site da TSI (www.telematica.com.br).

A nível País, atividades específicas de treinamento serão oferecidas a todos os funcionários (também através de *e-learning*) para assegurar a disseminação e correto entendimento do EGCP, das ASM, bem como das condutas relevantes para prevenção do cometimento de Crimes.

5. COMUNICAÇÃO A TERCEIROS

Terceiros serão informados dos princípios e conteúdo do TSIPG através de documentação contratual própria que deverá prever cláusulas padrão que, com base na atividade regulada pelo contrato, deverão ser vinculantes para a outra parte.

6. SISTEMA DISCIPLINAR

Medidas disciplinares apropriadas deverão ser aplicadas pelas funções competentes na hipótese de violação de qualquer norma de conduta estabelecida no EGCP, de acordo com o sistema disciplinar já em vigor, conforme as regras aplicáveis ou programas locais de compliance e sem prejuízo dos direitos concedidos aos empregados ao abrigo da legislação local (e.g. direito de defesa ou princípio do contraditório).

As medidas disciplinares deverão ser aplicadas independentemente dos resultados de qualquer procedimento criminal conduzido pela competente autoridade judicial.

A documentação contratual deverá prever sanções adequadas, incluindo, mas não limitadas à rescisão do contrato, de acordo com as leis aplicáveis, em caso de violação de qualquer disposição contida no EGCP por Terceiros.

7. CRIMES

O EGCP se aplica aos seguintes tipos de Crimes (doravante, "os Crimes", conforme abaixo descrito):

a. **Crimes de Suborno**
b. **Outros Crimes contra Autoridades Públicas**
c. **Fraude Contábil**
d. **Abuso de Mercado**
e. **Crimes de Financiamento do Terrorismo e Lavagem de Dinheiro**
f. **Crimes contra Pessoas**
g. **Crimes contra Saúde e Segurança**
h. **Crimes Ambientais**
i. **Crimes Cibernéticos**
j. **Crimes contra Direitos Autorais**

A Seção 9.2 abaixo do EGCP identifica as áreas de atividade a serem monitoradas pelos órgãos competentes e o principal padrão de conduta aplicável.

Portanto, os orgãos podem identificar:

i. as atividades de negócios que podem implicar risco específico de cometimento de um Crime através de uma análise dos processos de negócios e as possíveis formas decometimento atribuíveis aos tipos de ofensas;
ii. padrões adicionais de conduta que todos os Destinatários Corporativos e – quando expressamente especificado – Outros Destinatários têm que adotar de forma a:
    1. se absterem de qualquer conduta que enseje qualquer dos Crimes descritos acima; e
    2. se absterem de qualquer conduta que, ainda que emsi não constitua qualquer dos Crimes elencados acima, poderia potencialmente se transformar em um deles.

8. SISTEMA DE CONTROLE DO EGCP

O EGCP prevê os seguintes dois principais níveis de controle em relação às Áreas a Serem Monitoradas;

- normas gerais de controle;
- principais padrões de conduta aplicáveis a cada ASM.

9.1 NORMAS GERAIS DE CONTROLE

Os destinatários deveram cumprir a seguinte norma geral de controle:

- **segregação de funções**: a atribuição de funções, tarefas e responsabilidades dentro de uma célula é feitaem conformidade com a segregação de funções de acordo com a qual nenhum indivíduo pode realizar autonomamente um processo inteiro (ou seja, de acordo com este princípio, nenhum indivíduo pode ser autonomamente responsável pela realização de uma ação, autorização da mesma e, posteriormente, verificação da mesma); uma segregação adequada de funções também pode ser concedida utilizando sistemas de TI que permitam apenas a pessoas identificadas e autorizadas executar determinadas operações;
- **poder de assinatura e autorização**: devem existir regras formais acerca do exercício de poderes internos e poderes de assinatura. Os poderes de assinatura devem ser consistentes com as responsabilidades organizacionais e administrativas outorgadas a cada procurador dentro do órgão;
- **transparência e rastreabilidade de processos:** identificação e rastreabilidade de fontes, informações e controles executadas de forma a dar suporte à formação e implementação de decisões do grupo TSI, e a administração de recursos financeiros deve ser sempre garantida; armazenamento adequado de dados e informações relevantes deve ser garantido, através de sistemas de informações e/ou suporte de papel.
- **Administração adequada de relacionamentos com Terceiros:**

  - due diligence adequada de requisitos de honorabilidade antes do estabelecimento de qualquer relacionamento. A extensão de cada

avaliação de due diligence (o que pode incluir questionamentos através de contatos comerciais, câmaras de comércio locais, associações de negócios ou pesquisas de internet e follow up de referências comerciais e demonstrações financeiras) deve ser proporcional ao risco efetivo ou percebido de que qualquer potencial parceiro, consultor ou fornecedor possa não ter quaisquer dos requisitos acima mencionados; nesse sentido, as seguintes circunstâncias podem ser consideradas "bandeiras vermelhas"

- o terceiro é constituído em país que, de acordo com índices internacionais, como o Índice de Percepção de Corrupção da *Transparency International*, é conhecido por corrupção generalizada, ou em país considerado "país não cooperante" de acordo com a lista negra do FATF ou outra lista internacional preparada por instituições internacionais em relação à luta global contra o financiamento do terrorismo e lavagem de dinheiro;

- o terceiro esteja ou tenha sido suspenso de participar em licitações ou celebrar contrato com empresas estatais/órgão públicos/agências governamentais devido a investigações relativas a compliance realizadas pelas autoridades públicas;

- o terceiro já tenha sido sujeitado a processo criminal;

- o terceiro se recuse a cumprir o programa de compliance adotado pela companhia e não tenha nenhum código de conduta ou conjunto de regras semelhantes em vigor;

- o terceiro tenha relação familiar com um principal executivo de agência internacional ou com servidor público estrangeiro;

- um servidor público seja o dono, gerente administrativo ou um dos principais acionistas do terceiro;

- o endereço comercial do terceiro for umescritório virtual;

- o terceiro tenha um proprietário não revelado;

(i) verificações adicionais, na hipótese de, durante a fase de due diligence, ser identificada qualquer "bandeira vermelha";

(ii) monitoramento periódico durante o curso do

relacionamento para assegurar que a contraparte continua a preencher os requisitos aprovados pelo grupo TSI, e

(iii) medidas adequadas devem ser aplicadas na hipótese de um Terceiro não manter tais requisitos ou de qualquer outra "bandeira vermelha" surgir durante o curso do relacionamento contratual, como:

- o terceiro insista em tratar isoladamente com funcionários governamentais, não permitindo a participação da companhia;
- o terceiro solicite pagamentos antecipados incomuns;
- o terceiro ofereça submeter ou submeta faturas imprecisas ou faturas por serviços que não foram solicitados ou não foram executados;
- o terceiro solicite que pagamentos sejam efetuados em dinheiro ou instrumento ao portador;
- o terceiro solicite que pagamentos sejam efetuados fora de seu país de domicílio, em jurisdição que não tem qualquer relação com as entidades envolvidas na operação ou com a operação em si;
- o terceiro solicite que pagamentos sejam efetuados para um intermediário ou para outra entidade ou solicite que pagamentos sejam efetuados em duas ou mais contas bancárias;
- o terceiro solicite fundos a serem doados para instituição ou fundação sem fins lucrativos.

9.2 ÁREAS A SEREM MONITORADAS E PRINCIPAIS PADRÕES DE CONDUTA

A. Crimes de Suborno

Esse tipo de Crime refere-se a oferecer, dar, solicitar ou receber dinheiro (ou qualquer outro lucro, ganho ou vantagem) para fins ou com a intenção de influenciar aquele que recebe (que pode ser um indivíduo que faça parte de uma companhia privada ou um funcionário público) de qualquer forma que seja favorável para a parte que fornece o suborno.

Os subornos muitas vezes consistem de presentes ou pagamentos em dinheiro (outras formas de suborno podem incluir diversos bens, privilégios, entretenimento e favores) em troca de tratamento favorecido.

Tais tratamentos favorecidos, que ensejam o suborno, podem consistir, por exemplo, de:

- contratação do subornante para contrato relevante (seja com a administração pública ou com uma companhia privada);
- adjudicação de uma licitação pública;
- falso depoimento, favorável ao subornante, por testemunha em julgamento;
- relatório indulgente por parte de um funcionário público.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) negociação, assinatura e gestão de contratos relevantes com qualquer Parte (Autoridades Públicas, companhias, associações, fundações, etc.);

(ii) participação em licitações públicas ou privadas;

(iii) gestão de relacionamentos – diferente de relações contratuais – com organizações comunitárias e Autoridades Públicas (ex. em relação a requisitos de saúde, segurança e meio ambiente, administração de pessoal, pagamento de tributos);

(iv) gestão de disputas (ações judicias, arbitragens, procedimentos extrajudiciais);

(v) seleção de parceiros, intermediários e consultores e negociação, assinatura e gestão de contratos relevantes;

(vi) gestão de caixa e recursos financeiros;

(vii) gestão de iniciativas sem fins lucrativos;

(viii) gestão de despesas com presentes, entretenimento e hospitalidade;

(ix) reembolso de despesas incorridas por empregados;

(x) contratação de pessoal;

(xi) definição de incentivos de remuneração .

PRINCIPAIS PADRÕES DE CONDUTA

Ao conduzir negócios com companhias privadas, bem como com administrações públicas, governos internacionais, nacionais, estaduais e locais (as "**Autoridades Públicas**"), representantes estão comprometidos a agir com integridade e honestidade e deverão cumprir todas as leis e regulamentos aplicáveis.

Destinatários Corporativos e Terceiros (de acordo com termos contratuais específicos) ficam expressamente proibidos de:

a) oferecer dinheiro ou conceder outros benefícios de qualquer espécie (promessas de emprego, etc.) a representantes de Autoridades Públicas, bem como para indivíduos que façam parte de companhia privada – ou para membros de suas famílias (em conjunto, os "**Particulares**") – no caso de representantes de Autoridades Públicas, qualquer outro relacionamento, incluindo pedidos de fundos públicos, apresentação de qualquer autorização ouconsentimento público, etc.;

(i) outros presentes ou atividades de entretenimento aos indivíduos listados na letra a) acima, exceto o que for admitido de acordo com as práticas corporativas padrões. Presentes e benefícios de entretenimento permitidos incluem, mas não estão limitados a: (i) refeições ocasionais modestas; [(ii) presença ocasional em eventos esportivos locais, teatro e outros eventos culturais]; e (iii) presentes de baixo valor nominal como canetas, calendários ou outros pequenos itens promocionais. Presentes e benefícios de entretenimento não permitidos incluem, mas não estão limitados a: (i) viagens de fim de semana ou viagens de maior duração; (ii) presentes ou entretenimento que envolvam partes do grupo TSI esteja atualmente envolvida em uma licitação, concorrência ou outros procedimentos públicos. Presentes oferecidos – exceto aqueles de valor modesto – deverão ser documentados de forma a permitir as inspeções necessárias;

b) utilizar dinheiro como meio de pagamento exceto em casos permitidos pela regulação (ex. caixa pequeno);

c) incorrer quaisquer despesas promocionais ou de patrocínio, exceto quando tais despesas tenham sido aprovadas previamente por escrito pelo responsável

competente;

d) fazer quaisquer contribuições para instituições sem fins lucrativos, projetos de serviços comunitários e associações professionais, exceto quando tais contribuições tenham sido aprovadas previamente, por escrito, pelo responsável competente;

e) atribuir serviços a Terceiros que não sejam suficientemente justificados em relação às necessidades do grupo TSI;

f) pagar dinheiro a Terceiros que não esteja suficientemente justificado em relação ao tipo de atribuição a ser realizada e às práticas locais então vigentes.

B. Outros Crimes contra Autoridades Públicas

Este tipo de crime diz respeito principalmente à fraude contra entidades públicas e ocorre quando uma companhia utiliza um artifício ou outro esquema ilícito para desfraldar uma entidade pública ou para obter qualquer vantagem econômica através de declarações, promessas ou simulações falsas ou fraudulentas.

Tais tipos de Crimes estão muitas vezes ligados a financiamentos públicos e subsídios e ocorrem quando uma companhia reivindica financiamentos públicos ou subsídios para os quais não é elegível ou os utiliza indevidamente de forma diferente daquela prevista no respectivo acordo.

Este tipo de Crime pode ocorrer por diversas razões, as quais normalmente estão relacionadas à obtenção de vantagem econômica.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) Participação em licitações públicas e procedimentos públicos em geral;

(ii) Gestão de relacionamentos com Autoridades Públicas (ex. em relação a requisitos de saúde, segurança e meio ambiente, administração de pessoal, pagamento de tributos);

(iii) Aplicação de fundos públicos, outorgas, subsídios ou garantias concedidas por Autoridades Públicas;

(iv) Gestão de financiamentos públicos, outorgas, subsídios ou garantias recebidas.

PRINCIPAIS PADRÕES DE CONDUTA

Além dos principais padrões de conduta estabelecidos no parágrafo A) acima, os Destinatários Corporativos e Terceiros (de acordo com termos contratuais específicos) deverão abster-se de:

a) apresentar documentos falsos ou alterados, seja no todo ou em parte, durante a participação em licitações públicas;

b) induzir de qualquer forma Autoridades Públicas a realizarem avaliação ilícita durante a análise de pedidos de autorizações, licenças, liberações, concessões, etc.;

c) omitir informações necessárias de forma a direcionar de forma favorável para Autoridades Públicas em relação a quaisquer das circunstâncias descritas nas letras a)e b) acima;

d) qualquer conduta voltada para a obtenção de qualquer tipo de outorga, financiamento, empréstimo facilitado ou outros desembolsos da mesma natureza por parte de Autoridades Públicas, através de declarações e/ou documentos alterados ou falsificados, ou da omissão de informações relevantes ou, de forma geral, através de artifício ou fraude, com o objetivo de conduzir a instituição outorgante a erro;

e) utilizar dinheiro recebido de Autoridades Públicas, como fundos, contribuições ou empréstimos, para fins diversos daqueles para os quais os mesmos foram concedidos.

C. Fraude Contábil

A Fraude Contábil é um tipo de Crime que consiste principalmente em manipular intencionalmente demonstrações financeiras para criar uma falsa representação da saúde financeira de uma companhia para seus investidores, credores, acionistas e outras partes interessadas.

A Fraude Contábil pode ocorrer por diversas razões, incluindo mas não limitado a:

- continuar a obter financiamento de um banco (para esse fim, pode-se alterar as declarações financeiras de forma a criar uma representação de saúde financeira);
- reportar lucros não realísticos ou ocultar perdas;
- ocultar circunstâncias que poderiam afetar negativamente a companhia;
- causar inflação do preço da ação;
- disfarçar a criação de caixa dois;
- encobrir má conduta (tais como furto cometido pela administração da companhia);

- omissão de fatos relevantes que possa induzir em erro qualquer interessado (i.e. partes interessadas, credores, autoridades de bolsas de valores, etc.).

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) elaboração de documentos a serem divulgados para os acionistas ou para o público em geral (ex. demonstrações financeiras, relatórios financeiros periódicos) relativos aos ativos e passivos, receitas e despesas ou fluxos de caixa, ainda que tais documentos não sejam documentos contábeis periódicos;

(ii) gestão de relacionamentos com auditores externos e órgãos de supervisão.

PRINCIPAIS PADRÕES DE CONDUTA

O grupo TSI devem manter livros, registros e contas em nível razoável de detalhamento e de forma devida e precisa, que reflitam adequadamente as operações e alienação de ativos das companhias.

O grupo TSI devem avaliar a oportunidade de aplicar medidas adequadas e pessoal designado para manutenção de livros, registros e contas devem agir de forma apropriada paraassegurar que:

a) dados e informações utilizados para elaboração de relatórios financeiros periódicos sejam precisos e verificados de forma diligente;

b) todos os itens de balanço, cuja determinação e quantificação implica avaliações discricionárias, sejam objetivos e apoiados por documentação adequada;

c) as operações sejam executadas de acordo com as autorizações gerais ou específicas da administração;

d) as faturas e outra documentação relevante relativas às operações sejam devidamente analisadas, registradas e armazenadas;

e) as operações sejam registradas conforme necessário para permitir a elaboração de demonstrações financeiras em conformidade com os princípios contábeis aplicáveis ou geralmente aceitos ou qualquer outro critério aplicável a tais demonstrações;

f) acesso aos registros de tais operações seja permitido apenas de acordo com as autorizações gerais ou específicas da administração.

Ademais, de forma a assegurar que informações completas e justas sejam fornecidas ao mercado, o grupo TSI fica proibido de realizar qualquer conduta que impeça e, de qualquer forma, obstrua as atividades de verificação e auditoria por parte de auditores externos através da ocultação de documentos ou uso de outros meios fraudulentos.

D. Abuso de Mercado

Esta categoria de Crimes refere-se basicamente a três tipos de conduta diferentes: (1) vender ou comprar instrumentos financeiros utilizando informações que não estão disponíveispara o público ("**Informações Privilegiadas**") ou comunica-las de forma ilegítima a terceiros; (2) alterar o mecanismo de fixaçãode preço de instrumentos financeiros através da divulgação de informações sabidamente falsas ou enganosas de forma a influenciar o preço de um instrumento financeiro; (3) realizar ordens de compra e venda que forneçam ou visem (i) fornecer indicações falsas ou enganosas em relação à oferta, demanda ou preço de instrumentos financeiros, (ii) estabelecer o preço de mercado de um ou mais instrumentos financeiros em nível anômalo ou artificial.

Estes tipos de conduta podem ocorrer em benefício de uma companhia por diversas razões, incluindo, mas não limitado a:

- deflacionar o preço da ação de uma companhia alvo antes de uma aquisição;
- enfraquecer a reputação de uma companhia concorrente;
- alterar o preço de determinado instrumento financeiro em portfólio antes de realizar qualquer negociação relativa ao mesmo.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) gestão de informações públicas (ex. em relação a investidores, analistas financeiros e jornalistas e outros representantes da mídia de massa) e organização e participação em reuniões de qualquer tipo com tais pessoas;

(ii) gestão de Informações Privilegiadas relacionadas a companhias abertas e, especialmente, companhias abertas do Grupo e os respectivos instrumentos financeiros (por exemplo, novos produtos/serviços e mercados, informações contábeis do período, dados de previsão e metas quantitativas relativas a desempenho corporativo, fusões/cisões e, especialmente, novos negócios relevantes,

i.e., negociações e/ou acordos relativos à aquisição e/ou venda de ativos relevantes);

(iii) gestão de Informações Privilegiadas relativas a derivativos de energia (por exemplo, informações sobre indisponibilidade de usinas);

(iv) quaisquer tipos de informações relativas a instrumentos financeiros em portfólio.

PRINCIPAIS PADRÕES DE CONDUTA

Cada Destinatário fica expressamente proibido de:

a) utilizar Informações Privilegiadas para negociar, direta ou indiretamente, instrumentos financeiros a fim de obter vantagem pessoal, ou para favorecer Terceiros.

b) divulgar Informações Privilegiadas a Terceiros, exceto quando exigido por lei, ou outras disposições regulatórias ou contratos específicos em que as contrapartes estejam obrigadas a usar as informações apenas para os fins originalmente previstos e a manter confidencialidade sobre as mesmas;

c) recomendar ou induzir uma pessoa, com base em Informações Privilegiadas, a realizar qualquer tipo de operação envolvendo instrumentos financeiros.

Ademais, cada Destinatário fica expressamente proibido de:

d) espalhar informações falsas ou enganosas através da mídia (seja sobre a companhia em si ou sobre quaisquer outras companhias), incluindo a Internet, ou por quaisquer outros meios, apenas para alterar o processo, derivativos ou atividades subjacentes de uma ação que deem suporte a uma operação já planejada pela pessoa que espalha tais informações;

e) realizar quaisquer operações relativas a um instrumento financeiro (ex. compra ou venda) em violação dos regulamentos de abuso de mercado.

E. Crimes de Financiamento do Terrorismo e Lavagem de Dinheiro

O financiamento do terrorismo envolve a solicitação, coleta ou

fornecimento de fundos com a intenção de utilizá-los para apoiar atos ou organizações terroristas.

O principal objetivo de indivíduos ou entidades envolvidos no financiamento do terrorismo é ocultar tanto o financiamento como a natureza da atividade financiada.

A lavagem de dinheiro é o processo através do qual os proventos de uma atividade criminosa são disfarçados para ocultar sua origem ilícita. Mais precisamente, essa atividade pode englobar três condutas alternativas diferentes: (i) a conversão ou transferência de fundos, tendo conhecimento de que são proventos de um crime (ii) ocultar ou disfarçar a verdadeira natureza, fonte, localização, disposição, movimentação ou propriedade de ou direitos relativos à propriedade tendo conhecimento de que são proventos de um crime; e (iii) a aquisição, posse ou uso de propriedade, tendo conhecimento, quando do recebimento, de que tal propriedade é provento de um crime.

Quando os proventos de um crime são criados pela mesma pessoa que está ocultando a origem ilícita dos mesmos, tal conduta é punível em alguns países como autolavagem de dinheiro.

A lavagem de dinheiro e o financiamento do terrorismo muitas vezes têm características operacionais semelhantes, principalmente no que se refere ao ocultamento. Os indivíduos que lavam dinheiro remetem fundos ilícitos através de canais legais de forma a ocultar suas origens criminosas, enquanto aqueles que financiam o terrorismo transferem fundos que podem ser legais ou ilícitos em origem, de tal forma a ocultar sua fonte e utilização final, que é o apoio ao terrorismo.

Estes tipos de conduta podem ocorrer em benefício da companhia por diversas razões, incluindo, mas não limitado a:

- obter proventos ou qualquer outra vantagem resultante de atividades ilegais realizadas pelas organizações terroristas que foram financiadas (as outras vantagens podem consistir da proteção do negócio, em países em que tais organizações são muito influentes);
- disfarçar a origem ilegal de proventos do crime.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) operações financeiras ou comerciais realizadas com indivíduos ou empresas – e entidades legais controladas direta ou indiretamente pelas partes acima mencionadas – que tenham residência ou sede social em países que representam jurisdição de alto risco e não cooperativas (i.e. com deficiências estratégicas em sua estrutura para o combate da proliferação de lavagem de dinheiro e financiamento do terrorismo) de acordo com a avaliação de autoridades internacionais.

F. Crimes contra Pessoas

O termo "crimes contra pessoas" refere-se a diversos tipos de ofensas criminais que geralmente envolvem lesões pessoais, ameaça de danos corporais, ou outras ações cometidas contra a vontade de uma pessoa.

No entanto, para fins deste TSIPG, Crimes contra Pessoas referem-se principalmente aos crimes que podem ocorrer com maior probabilidade na gestão de uma companhia, como os que se referem a práticas de trabalho forçado, consistindo principalmente em coagir os empregados a trabalharem através do uso de violência ou intimidação ou por outros meios como a retenção de documentos de identidade.

Este tipo de Crime pode ocorrer por diversas razões, incluindo, mas não limitado a:

- empregar mão-de-obra com despesas mínimas;
- empregar mão-de-obra totalmente subserviente, para qual nenhum pedido seria recusado.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) celebração de contratos com fornecedores que utilizam profissionais não qualificados e/ou que operam em países em que direitos individuais não são totalmente protegidos por leis internacionais ou locais.

G. Crimes contra Saúde e Segurança

Crimes contra a saúde e segurança são relacionados principalmente ao descumprimento de leis locais e normas trabalhistas a serem implementadas no local de trabalho de forma a evitar acidentes e doenças dos trabalhadores.

Esses tipos de condutas podem ocorrer em benefício de uma companhia por diversas razões, incluindo, mas não limitado a:

- reduzir custos, já que a adoção das medidas exigidas muitas vezes resulta em despesas adicionais para a companhia;
- aumentar a produtividade, já que trabalhar sem levar em conta procedimentos e políticas de precaução pode acelerar o processo de produção.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) cumprimento de leis relativas à saúde e segurança.

PRINCIPAIS PADRÕES DE CONDUTA

Não obstante a dimensão local da legislação local relativa à saúde e segurança no local de trabalho, a TSI deve promover e reforçar uma cultura forte de proteção da segurança no local de trabalho, aumentando a consciência acerca de riscos e responsabilidades de condutas individuais.

Para este fim, não obstante o cumprimento da legislação local aplicável acerca de saúde e segurança no local de trabalho, a TSI está comprometida a adotar todas as medidas necessárias, de forma a proteger a integridade física e moral dos trabalhadores.

Em especial, a TSI deve assegurar que:

a) o respeito às disposições legais que governam a saúde e segurança dos trabalhadores no local de trabalho seja uma prioridade;

b) o risco para trabalhadores, na medida do possível e permitido pela evolução das melhores técnicas, sejam avaliados com o objetivo de proteção, e também pela escolha dos materiais e equipamentos mais apropriados e seguros, de forma a reduzir o risco na fonte;

c) os riscos não evitáveis sejam avaliados corretamente e mitigados de forma adequada através das medidas de segurança individuais e coletivas adequadas;

d) a informação e treinamento dos trabalhadores seja disseminada, atualizada e específica no que se refere à atividade desenvolvida;

e) os trabalhadores sejam ouvidos periodicamente acerca de assuntos relativos à saúde e segurança no local de trabalho;

f) qualquer área de não cumprimento ou melhoria, surgida durante a atividade de trabalho ou durante inspeções, seja levada em consideração de forma tempestiva e efetiva;

g) a organização da atividade de trabalho seja estruturada de forma a proteger a integridade dos trabalhadores, de Terceiros e da comunidade em que a TSI opera.

Para conseguir o acima descrito, a TSI atribui recursos organizacionais, instrumentais e econômicos tanto para assegurar o total cumprimento das disposições legais em vigor acerca da prevenção de acidentes industriais e para melhorar continuamente a saúde e segurança dos trabalhadores no local de trabalho e respectivas medidas preventivas.

Os Destinatários Corporativos, cada um de acordo com seu papel dentro da organização, devem assegurar total respeito às disposições legais, procedimentos corporativos e quaisquer outros regulamentos internos voltados para a proteção da saúde e segurança dos trabalhadores no local de trabalho.

H. Crimes Ambientais

Crimes Ambientais referem-se a uma vasta lista de atividades ilícitas, incluindo o comércio ilegal de animais selvagens, crimes de gestão de água, comércio ilícito e eliminação de substâncias perigosas, e contrabando de substâncias que destroem a camada de ozônio.

Os Crimes Ambientais normalmente afetam a qualidade do ar, água e solo, ameaçam a sobrevivência de espécies e podem causar desastres incontroláveis e apresentar ameaça à segurança de um enorme número de pessoas.

Induzidos por enormes ganhos financeiros e facilitados por um baixo risco de detecção e escassas taxas de condenação, as redes criminosas e os grupos criminosos organizados estão cada vez mais interessados em tais atividades ilícitas e frequentemente transnacionais.

Estes tipos de conduta podem ocorrer em benefício da companhia por diversas razões, incluindo, mas não limitado a:

- reduzir custos, já que a adoção de medidas necessárias para proteção do meio ambiente muitas vezes resultam em despesas adicionais;
- aumentar a produtividade, considerando que trabalhar sem levar em conta questões ambientais pode acelerar o processo de produção.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) observância das leis ambientais aplicáveis relativas ao

desenho, construção, gestão e manutenção de infraestruturas relacionadas.

PRINCIPAIS PADRÕES DE CONDUTA

Em seus negócios, a TSI deve seguir o princípio de proteção do meio ambiente.

Especialmente, deve:

a) contribuir para a disseminação e aumento de conscientização acerca da proteção do meio ambiente e administra as atividades que lhe são confiadas, em conformidade com a legislação aplicável;

b) promover desenvolvimento científico e tecnológico voltado para a proteção do meio ambiente e recursos através da adoção, em suas operações, de sistemas avançados de proteção do meio ambiente e eficiência energética;

c) trabalhar para satisfazer as expectativas dos seus clientes/interessados em relação às questões ambientais e adotar todos os instrumentos adequados de proteção e preservação e condenar qualquer forma de danos ao ecossistema.

Nos acordos celebrados com Terceiros nos quais possa surgir a responsabilidade da Companhia nos termos da legislação ambiental, especialmente no que diz respeito à gestão e eliminação de resíduos, a Companhia deverá incluir disposições que imponham a tais Terceiros o cumprimento das leis aplicáveis e prevejam sanções contratuais no caso de violação.

I. Crimes Cibernéticos

Crimes Cibernéticos são delitos que envolvem duas categorias distintas de crimes: um em que o alvo é a rede ou um computador e outro em que os crimes são cometidos ou acelerados por um computador.

Para fins do TSIGP, Crimes Cibernéticos não incluem aqueles crimes que podem ser facilitados por um crime informático, tais como fraude, roubo, chantagem, falsificação e assédio (por exemplo, *cyber-bullying* ou *cyber-stalking*).

Portanto, os Crimes Cibernéticos considerados pelo TSIGP consistem, por exemplo, de: (i) intrusão não autorizada em uma rede protegida; (ii) introdução de vírus de computador em um sistema de computadores; (iii) intercepção de dados de uma rede de computadores.

Os Crimes Cibernéticos podem ocorrer por diversas razões, incluindo, mas não limitado a:

- roubar segredos comerciais de um competidor;
- prejudicar ou danificar o sistema informático de um competidor;
- obter informações confidenciais acerca das estratégias de mercado de um competidor.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) atividades da companhia executadas por Destinatários utilizando a Intranet, Internet, sistema de e-mails ou outros instrumentos de TI;

(ii) gestão e proteção de estações de trabalho;

(iii) gestão de dispositivos de armazenamento;

(iv) planejamento das medidas a serem adotadas em sistemas telemáticos e segurança, classificação e processamento de informações e dados;

(v) gestão do perfil dos administradores do sistema.

PRINCIPAIS PADRÕES DE CONDUTA

A TSI deve avaliar a oportunidade de aplicarem medidas técnicas, físicas e organizacionais adequadas de forma a evitar, e cada Destinatário fica obrigado a não incorrerem:

a) uso indevido de credenciais de TI;
b) acesso ilícito de Terceiros aos sistemas de TI;
c) compartilhamento não autorizado de informações comerciais fora da companhia;
d) uso de dispositivos pessoais ou não autorizados para transmitir ou armazenar informações ou dados da companhia;
e) adulteração ou alteração do sistema informático;
f) extração ilícita de dados;
g) adulteração, furto ou destruição dos ativos informáticos (arquivos, dados e programas);
h) uso de quaisquer falhas nas medidas de segurança do sistema de informações corporativas para acessar informações sem autorização adequada;

i) práticas de spam;
j) acesso aos sistemas informáticos através de dispositivos externos (computador pessoal, periféricos, hard drives externos, etc.) e instalação de softwares e bases de dados sem prévia autorização;
k) instalação de software danoso (ex. *worms* e vírus);
l) uso de software e/ou hardware não autorizado que possa ser utilizado para avaliar ou comprometer a segurança dos sistemas de computador (ex. sistemas para identificar as credenciais, descriptografar arquivos criptografados, etc.).

A TSI, de forma a identificar condutas anormais, potenciais vulnerabilidades e deficiências nos sistemas corporativos, deve assegurar monitoramento periódico das atividades desenvolvidas pelo destinatário e/ou terceiros no sistema corporativo de TI, de acordo com as leis locais aplicáveis.

J. Crimes contra Direitos Autorais

A violação de direitos autorais pode consistir na utilização de trabalhos (ex. softwares, bases de dados, vídeos, imagens) protegidos pela lei de direitos autorais sem permissão, violando determinados direitos outorgados ao detentor dos direitos autorais, incluindo, mas não limitado ao direito de usar, distribuir ou desenvolver trabalhos derivados.

Para fins do TSIGP, Crimes contra Direitos Autorais referem-se principalmente àqueles crimes que podem mais facilmente ser contemplados na administração de uma companhia, tais como os relativos ao uso ilegal de softwares e bases de dados.

Este tipo de Crime pode ocorrer por diversas razões, incluindo, mas não limitado a:

- reduzir custos através do não pagamento de licenças de software.

ÁREAS A SEREM MONITORADAS

Em relação a este tipo de Crime, as seguintes áreas devem ser monitoradas:

(i) atividades da companhia desenvolvias por Destinatários utilizando a Intranet e qualquer ferramenta de TI fornecida pela TSI.

PRINCIPAIS PADRÕES DE CONDUTA

Além dos principais padrões de conduta estabelecidos no parágrafo 9.2 seção I) acima, a TSI deverá avaliar a oportunidade de adotar medidas técnicas,físicas e organizacionais de forma a evitar:

1. qualquer uso ou disseminação ilegal para o público, através de redes baseadas em computadores ou através de conexão de qualquer tipo, de trabalhos originais protegidos, ou parte dos mesmos;
2. uso, distribuição, extração, venda ou arrendamento do conteúdo de base de dados em violação do direito exclusivo de execução e autorização do detentor dos direitos autorais;
3. download ilegal de qualquer software sem a assinatura da documentação contratual apropriada;
4. o download de software entre pares (*peer to peer*) ou qualquer outro software não ligado diretamente à atividade corporativa.