Programa Global de *Compliance* relativo à responsabilidade corporativa

Índice

Introdução 4

1. Missão 6

2. Estrutura 8

3. Adoção, implementação e aditivos subsequentes 10

4. Disseminação do EGCP e atividades de treinamento 12

5. Comunicação a terceiros 14

6. Sistema disciplinar 16

7. Infrações 18

8. Sistema de controle do EGCP 20

8.1. Normas gerais de controle 21

8.2. Áreas a serem monitoradas e principais padrões de conduta 23

A. Suborno 23
B. Outros Atos Lesivos contra Autoridades Públicas 26
C. Fraude Contábil 28
D. Violação contra a Defesa da Concorrência 30
E. Financiamento ao Terrorismo e Lavagem de Dinheiro 32
F. Crimes contra Pessoas 34
G. Crimes contra Saúde e Segurança 35
H. Crimes Ambientais 37
I. Crimes Cibernéticos 38
J. Crimes contra Direitos Autorais 40

Anexo 1
Exemplos de condutas ilegais cometidas na ASM 42

Introdução

A Enel Brasil S.A. ("Enel") é a holding de um grupo multinacional que atua em um setor de negócios complexo, altamente regulado e em diferentes ambientes econômicos, políticos, sociais e culturais.

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, ética, transparência e em estrito cumprimento das leis e dos regulamentos, nacionais e estrangeiros, das normas e diretrizes internacionais.

*O "***Programa Global de *Compliance* Enel**" (*Enel Global Compliance Program* ou "**EGCP**") foi concebido como uma ferramenta para reforçar o compromisso da Enel com os mais elevados padrões éticos, legais e profissionais para o aprimoramento e a preservação da reputação do grupo. Para esse fim, o programa estabelece uma série de medidas preventivas relativas à responsabilidade criminal corporativa.

Nos últimos anos, vem aumentando o número de países que estabeleceram um processo de responsabilidade corporativa, permitindo que tribunais penalizem também as pessoas jurídicas por condutas praticadas por parte de seus representantes, empregados ou terceiros atuando em seu nome.

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

O EGCP, 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**" – que estejam respectivamente empregados ou nomeados ou que tratem com ou atuem em nome das subsidiárias não italianas (as "**Subsidiárias Não Italianas**" ou "**SNI**").

O EGCP aplica-se globalmente a todas as SNI de acordo com a governança legal e corporativa, bem como com as diferenças culturais, sociais e econômicas dos diversos países em que as SNI operam.

Na hipótese de conflitos entre o ECGP e outras normas privadas ou técnicas, o EGCP deverá prevalecer.

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

1. Missão

O EGCP representa uma oportunidade de reforçar a prevenção proativa de responsabilidade corporativa por meio 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 EGCP identifica os principais padrões de conduta esperados de todos os Destinatários Corporativos e – quando especificado – dos Outros Destinatários, no intuito de:

i. Fornecer às SNI um conjunto de regras destinadas a prevenir uma responsabilidade corporativa no respectivo país;

ii. Integrar o programa local de *compliance* adotado por uma SNI, de acordo com qualquer lei sobre responsabilidade criminal corporativa aplicável.

As regras contidas no EGCP são integradas:

i. Pelas disposições estabelecidas no Código de Ética que representam os princípios éticos do grupo, os quais todos os Destinatários são obrigados a cumprir;

ii. Pelas disposições estabelecidas no Plano de Tolerância Zero com a Corrupção adotado por todo o grupo Enel;

iii. Pelas disposições de governança corporativa adotadas pelas SNI, refletindo as leis aplicáveis e as melhores práticas internacionais;

iv. Pelo sistema de controle interno adotado pelas SNI;

v. Pelas disposições estabelecidas em qualquer programa local de *compliance* adotado por uma SNI, a fim de cumprir as suas próprias leis locais relativas à responsabilidade corporativa e em quaisquer diretrizes, políticas ou documentos organizacionais internos correlatos.

2. Estrutura

EGCP identifica:

a. As modalidades de sua adoção pelas SNI e o respectivo processo de atualização;

b. A sua disseminação para os Destinatários e as atividades de treinamento;

c. O sistema disciplinar aplicável, em caso de violação de qualquer disposição contida nele;

d. Normas gerais de controle;

e. Áreas de atividade a serem monitoradas em relação a certos tipos de conduta ilícitos (as "**Áreas a Serem Monitoradas**" ou "**ASM**"), conforme elencadas na Seção 7, que, geralmente, são consideradas infrações e podem potencialmente ser cometidas por uma SNI, e a prevenção das quais a Enel considera uma prioridade para a condução de seus negócios, com honestidade e integridade (as "**Infrações**");

f. Principais padrões de conduta ligados às áreas a serem monitoradas.

O EGCP é completado pelo Anexo 1, relativo a "Exemplos de condutas ilícitas cometidas na ASM".

3. Adoção, implementação e aditivos subsequentes

O EGCP foi aprovado pelo Conselho de Administração da Enel, em 15/12/2016, e deverá ser aprovado pelo Conselho de Administração, ou outro órgão de administração, da SNI.

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

i. Adota as medidas mais adequadas para a implementação e o monitoramento do EGCP, levando em consideração o tamanho, a complexidade das atividades desenvolvidas, o sistema de controles internos, o perfil de risco específico da respectiva SNI e seu quadro regulatório;

ii. É responsável pela implementação adequada das áreas a serem monitoradas e dos principais padrões de conduta, conforme estabelecido na seção 8.2 do EGCP, bem como dos controles determinados pelo Programa Global de *Compliance* da Enel.

O EGCP deverá ser aplicado pela SNI de acordo com a legislação aplicável, os tipos de negócios desenvolvidos, bem como as características específicas de sua estrutura organizacional.

Outras alterações substanciais e aditamentos ao EGCP serão de responsabilidade do Conselho de Administração da Enel e, posteriormente, serão aprovados pelo Conselho de Administração ou por outro órgão de administração das SNI.

Cada SNI deverá relatar mudanças ou interpretações específicas realizadas de acordo com as leis e os costumes locais.

O Conselho de Administração/órgão de administração da SNI deverá identificar a estrutura (indivíduo ou órgão) responsável por dar suporte à implementação e ao monitoramento do EGCP e por executar os controles relacionados.

Um sistema específico de notificação de violações suspeitas ou conhecidas do EGCP deverá ser identificado pela SNI.

4. Disseminação do EGCP e atividades de treinamento

O EGCP estará disponível e o *download* poderá ser efetuado na intranet do grupo Enel.

Serão oferecidas atividades específicas de treinamento a todos os funcionários (também, por meio de *e-learning*) para assegurar a disseminação e o entendimento correto do EGCP, das ASM, bem como das condutas relevantes para a prevenção do cometimento de infrações. Tais treinamentos também podem ser organizados no contexto de qualquer programa adotado por uma SNI, em relação ao cumprimento de leis e programas locais de *compliance*.

5. Comunicação a terceiros

Os Terceiros serão informados dos princípios e sobre o conteúdo do EGCP por meio de documentação contratual própria, que deverá prever cláusulas padrão vinculantes para o Terceiro, de acordo com o objeto do contrato.

6. Sistema disciplinar

Na hipótese de violação de qualquer norma de conduta estabelecida no EGCP, as funções competentes das SNI deverão aplicar medidas disciplinares apropriadas, de acordo com o sistema disciplinar já em vigor, conforme as regras aplicáveis ou os programas locais de *compliance* e sem prejuízo dos direitos concedidos aos empregados, conforme disposto na legislação local (e.g. direito de defesa ou princípio do contraditório).

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

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

7. Infrações

O EGCP se aplica aos seguintes tipos de delitos, conforme descrito abaixo:

A. Suborno

B. Outros Atos Lesivos contra Autoridades Públicas

C. Fraude Contábil

D. Violação contra a Defesa da Concorrência

E. Financiamento ao 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 8.2 do EGCP identifica as áreas de atividade a serem monitoradas pelas SNI e o principal padrão de conduta aplicável.

A lista incluída no parágrafo 8.2 não exime as SNI de realizarem a sua própria avaliação de risco e definirem os principais padrões de conduta, caso seja considerado necessário.

Portanto, a SNI pode identificar:

i. As atividades de negócios que podem implicar em risco específico de prática de uma infração por meio de uma análise dos processos e as possíveis formas em que a infração pode ocorrer;

ii. Padrões adicionais de conduta que todos os Destinatários Corporativos e – quando expressamente especificado – Outros Destinatários têm que adotar de maneira a:

— Se absterem de qualquer conduta que enseje qualquer das infrações descritas acima, inclusive a conduta de não reportar uma situação que seja ou aparente ser uma das infrações elencadas acima;

— Se absterem de qualquer conduta que, ainda que em si não constitua nenhuma das infrações elencadas acima, potencialmente poderia se transformar em uma delas.

8. Sistema de controle do EGCP

O EGCP prevê os seguintes níveis de controle principais em relação às áreas a serem monitoradas:

— Normas gerais de controle

— Principais padrões de conduta aplicáveis a cada ASM

8.1. NORMAS GERAIS DE CONTROLE

A SNI deverá cumprir a seguinte norma geral de controle:

— **Segregação de funções**: a atribuição de funções, tarefas e responsabilidades dentro de uma SNI é feita em conformidade com a segregação de funções de acordo com a qual nenhum indivíduo pode realizar autonomamente um processo inteiro (ou seja, de acordo com esse princípio, nenhum indivíduo pode ser exclusivamente responsável pela realização, autorização e, posteriormente, verificação de uma ação de maneira autônoma). Uma segregação adequada de funções também pode ser concedida utilizando sistemas de TI que permitam que apenas pessoas identificadas e autorizadas executem determinadas operações.

— **Poder de assinatura e autorização**: devem existir regras formais acerca do exercício de poderes internos e de assinatura. Os poderes de assinatura devem ser consistentes com as responsabilidades organizacionais e administrativas outorgadas a cada procurador dentro da SNI.

— **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 da SNI, e a administração de recursos financeiros deve ser sempre garantida. Armazenamento adequado de dados e informações relevantes deve ser garantido, por meio de sistemas de informações e/ou suporte de papel.

— **Gerenciamento adequado de relacionamentos com Terceiros**

i. *Due diligence* adequada de requisitos de integridade, antes de firmar qualquer relacionamento. A extensão de cada avaliação de *due diligence* – que pode incluir questionamentos por meio de contatos comerciais, câmaras de comércio locais, associações de negócios ou pesquisas de internet e acompanhamento 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 sinais de alertas:

— O Terceiro é constituído em país que, de acordo com índices internacionais, como o Índice de Percepção de Corrupção da Transparência Internacional, é conhecido por corrupção generalizada, ou em local considerado "país não cooperante", de acordo com a lista do FATF (*Financial Action Task Force*) ou outra lista preparada por instituições internacionais em relação à luta global contra o financiamento do terrorismo e a 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 um processo criminal ou civil e administrativo por atos praticados contra a administração pública;

— O Terceiro se recuse a cumprir o programa de *compliance* adotado pela companhia e não possua padrões de condutas em vigor;

— O Terceiro possui relação familiar com um executivo de órgão governamental ou um servidor público estrangeiro;

— Um servidor público seja o dono, gerente administrativo ou um dos principais acionistas do Terceiro;

— O endereço comercial do Terceiro seja um escritório virtual;

— O Terceiro possua um sócio ou beneficiário não revelado.

ii. Verificações adicionais, na hipótese de, durante a fase de *due diligence*, serem identificados quaisquer sinais de alerta;

iii. Monitoramento periódico durante o curso do relacionamento para assegurar que a contraparte continua preenchendo os requisitos aprovados pela SNI;

iv. 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 se ofereça para 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 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.

8.2. ÁREAS A SEREM MONITORADAS E PRINCIPAIS PADRÕES DE CONDUTA

A. Suborno

Esse tipo de delito refere-se a oferecer, dar, solicitar ou receber qualquer coisa de valor e/ou vantagem indevida para ou com a intenção de influenciar aquele que recebe, que pode ser um funcionário público ou não, ou ser influenciado de qualquer forma que seja favorável para si ou para a outra parte.

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

Tais tratamentos, que ensejam o suborno, podem equivaler, por exemplo, a:

— Contratação daquele que oferece suborno para um contrato relevante (seja com a administração pública ou uma empresa privada);

— Adjudicação de uma licitação pública;

— Depoimento falso ou favorável, por testemunha, em julgamento em que a pessoa que oferece o suborno é parte;

— Relatório impreciso por parte de um funcionário público.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de infração, 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 (por exemplo, em relação a requisitos de saúde, segurança e meio ambiente, administração de pessoal, pagamento de tributos);

iv. Gestão de disputas (ações judiciais, 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 (por exemplo, Gestão por Objetivos - MBOs) voltados para executivos.

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

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

a. Oferecer, dar, solicitar ou receber qualquer coisa de valor e/ou vantagem indevida para ou com a intenção de influenciar autoridades públicas, bem como para indivíduos que façam parte de empresa privada – ou para membros de suas famílias (em conjunto, os "**Particulares**") – com quem a SNI pretenda iniciar ou já conduza uma relação de negócios ou, no caso de autoridades públicas, qualquer outro relacionamento, incluindo pedidos de fundos públicos, apresentação de qualquer autorização ou consentimento público, etc.;

b. Oferecer presentes ou atividades de entretenimento às autoridades públicas, exceto o que for admitido de acordo com as práticas corporativas padrão, as leis locais e as normas aplicáveis às autoridades públicas. Presentes e 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) brindes institucionais, como canetas, calendários ou outros itens promocionais. Presentes e benefícios de entretenimento não permitidos incluem, mas não estão limitados a: (i) viagens de fim de semana ou de maior duração; (ii) presentes ou entretenimento que envolvam partes com quem a SNI ou qualquer outra companhia do grupo Enel 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;

c. Utilizar dinheiro como meio de pagamento, exceto em casos de taxas permitidas pela regulação, determinadas pelos órgãos públicos;

d. Incorrer em quaisquer despesas promocionais ou de patrocínio, exceto quando tais despesas tenham sido aprovadas previamente, por escrito, pelo responsável competente;

e. 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;

f. Atribuir serviços a Terceiros que não sejam suficientemente justificados em relação às necessidades da SNI;

g. Pagar dinheiro a Terceiros sem justificativa suficiente em relação ao tipo de atribuição a ser realizada e às práticas locais vigentes;

As SNI deverão avaliar a oportunidade para adoção das medidas organizacionais adequadas para prevenir que um Destinatário realize qualquer das atividades descritas acima. Ademais, as SNI deverão avaliar a oportunidade para adoção de procedimentos adequados a fim de assegurar que:

h. Provas adequadas sejam dadas em relação a quaisquer relacionamentos relevantes com autoridades públicas (por exemplo, procedimentos administrati-

vos que objetivem a obtenção de uma autorização, licença ou ato semelhante, *joint ventures* com entidades públicas, apresentação de pedido para obtenção de determinada autorização pública);

i. Relacionamentos com autoridades públicas, quando assuntos relativos aos interesses da SNI estiverem em jogo, sejam geridos por, pelo menos, duas pessoas autorizadas;

j. Todo procedimento de recrutamento seja realizado apenas com base em uma necessidade comercial real e demonstrável, o processo de seleção envolva pelos menos dois cargos distintos e tenha por base critérios de objetividade, competência e profissionalismo, com a intenção de evitar favoritismo ou nepotismo e conflitos de interesses;

k. Planos de incentivos dos executivos sejam adotados de forma que assegurem que os objetivos estabelecidos não resultem em conduta abusiva e sejam, em vez disso, focados em um possível resultado determinado, mensurável e relacionado ao tempo necessário para atingi-los;

l. Em relação ao planejamento de projetos, sejam estabelecidos prazos realistas;

m. Em relação ao reembolso de despesas, a documentação adequada, incluindo recibos originais que deem suporte ao pagamento das despesas ou que incorreram no custo, deve ser apresentada ao departamento contábil apropriado antes do pagamento, e o pagamento ou despesa subsequente (ou recebimento do mesmo) deve estar descrito de forma precisa e refletida nos registros contábeis da respectiva SNI.

B. Outros Atos Lesivos contra Autoridades Públicas

Esse tipo de delito diz respeito principalmente a atos contra entidades públicas e ocorre quando a empresa utiliza um artifício ou qualquer outra forma indevida para prejudicar uma entidade pública ou para obter uma vantagem indevida por meio de declarações, promessas ou simulações.

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

Pode ocorrer por diversas razões, as quais normalmente estão relacionadas à obtenção de vantagem indevida.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de infração, as seguintes áreas devem ser monitoradas:

i. Participação em licitações e procedimentos públicos em geral;

ii. Gestão de relacionamentos com autoridades públicas (por exemplo, em relação a requisitos de saúde, segurança e meio ambiente, administração de pessoal, pagamento de tributos);

iii. Solicitação 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 na cláusula "8.2 A" acima, os Destinatários Corporativos e Terceiros, de acordo com os 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 incorreta durante a análise de pedidos de autorizações, licenças, liberações, concessões, etc.;

c. Omitir informações necessárias de maneira a direcionar favoravelmente para a SNI decisões de autoridades públicas em relação a quaisquer 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, por meio de declarações e/ou documentos alterados ou falsificados, ou da omissão de informações relevantes ou, de forma geral, por meio de artifício ou fraude, com o objetivo de conduzir a instituição outorgante ao erro;

e. Utilizar dinheiro recebido de autoridades públicas, como fundos, contribuições ou empréstimos, para fins diversos daqueles para os quais foram concedidos.

Além disso, de forma a implementar os padrões de comportamento descritos acima, as SNI deverão avaliar a oportunidade para adoção de medidas organizacionais adequadas, a fim de assegurar que:

a. Todas as declarações apresentadas a autoridades públicas, nacionais ou

internacionais, para fins de obtenção de fundos, outorgas ou empréstimos incluam apenas informações verdadeiras e sejam assinadas por signatários autorizados, e quando da obtenção de tais fundos, outorgas ou empréstimos, sejam devidamente contabilizados;

b. Controles para segregação adequada de funções estejam em vigor, assegurando que as fases de pedido, gestão e reporte – relativas a procedimentos públicos para fins de obtenção de fundos, outorgas ou empréstimos – sejam administradas por diferentes Destinatários Corporativos dentro da organização;

c. As atividades de coleta e análise de informações necessárias para fins de relatório sejam realizadas com o suporte das funções competentes;

d. A documentação e o subsequente relatório a serem submetidos em relação à necessidade de pedido de subsídios, outorgas, empréstimos e garantias sejam aprovados por níveis hierárquicos apropriados.

C. Fraude Contábil

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

Pode ocorrer por diversas razões, incluindo, mas não se limitando 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 possam induzir a erro qualquer interessado (partes interessadas, credores, autoridades de bolsas de valores, etc.).

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de infração, as seguintes áreas devem ser monitoradas:

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

ii. Gestão de relacionamentos com auditores externos e órgãos de supervisão.

Principais padrões de conduta
As SNI devem manter livros, registros e contas em um nível razoável de detalhamento e de forma devida e precisa, que reflitam adequadamente as operações e a alienação de ativos das companhias, assegurando 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 implicam avaliações discricionárias, sejam objetivos e apoiados por uma documentação adequada;

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

d. As faturas e outras documentações relevantes relativas às operações sejam devidamente analisadas, registradas e armazenadas;

e. As operações sejam registradas, de acordo com o 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. Seja permitido o acesso aos registros de tais operações apenas de acordo com as autorizações gerais ou específicas da administração.

Ademais, de forma a assegurar que sejam fornecidas ao mercado informações completas e justas, as SNI ficam proibidas de realizar qualquer conduta que impeça e, de qualquer maneira, obstrua as atividades de verificação e auditoria por parte de auditores externos por meio da ocultação de documentos ou uso de outros meios fraudulentos.

Finalmente, as SNI devem efetuar todas as comunicações dirigidas a qualquer autoridade pública financeira (conforme previsto na lei local aplicável) da maneira correta, completa, devida e célere, não impedindo, de nenhum jeito, que desempenhem suas funções, mesmo no contexto de uma inspeção (por exemplo, oposição expressa, recusa injustificada, conduta obstrutiva ou falha em cooperar).

D. Violação contra a Defesa da Concorrência

Essa categoria refere-se basicamente a três tipos diferentes de conduta: (1) vender ou comprar instrumentos financeiros utilizando informações que não estão disponíveis para o público ("**Informações Privilegiadas**") ou comunicá-las de forma ilegítima a terceiros; (2) alterar o mecanismo de fixação de preço de instrumentos financeiros por meio da divulgação de informações sabidamente falsas ou enganosas para 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 ao preço de instrumentos financeiros, (ii) estabelecer o preço de mercado de um ou mais instrumentos financeiros em nível anômalo ou artificial.

Esses tipos de conduta podem ocorrer em benefício de uma companhia por diversas razões, incluindo, mas não se limitando 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 um determinado instrumento financeiro em portfólio antes de realizar qualquer negociação relativa a ele.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de infração, as seguintes áreas devem ser monitoradas:

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

ii. Gestão de informações privilegiadas relacionadas a companhias abertas e, particularmente, 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, uma SNI ou qualquer outra companhia do grupo;

b. Divulgar informações privilegiadas a Terceiros, exceto quando exigido por lei, 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 a confidencialidade sobre elas;

c. Recomendar ou induzir uma pessoa, com base em informações privilegiadas, a realizar qualquer tipo de operação envolvendo instrumentos financeiros.

d. Espalhar informações falsas ou enganosas por meio 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, os derivativos ou as atividades subjacentes de uma ação que dê suporte a uma operação já planejada pela pessoa que dissemina tais informações;

e. Realizar quaisquer operações relativas a um instrumento financeiro (por exemplo, compra ou venda) em violação dos regulamentos de abuso de mercado.

E. Financiamento ao Terrorismo e Lavagem de Dinheiro

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

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

Quando os proventos de uma infração são criados pela mesma pessoa que está ocultando a sua origem ilícita, tal conduta é punível em alguns países, como autolavagem de dinheiro.

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

Esses tipos de conduta podem ocorrer em benefício da companhia por diversas razões, incluindo, mas não se limitando a:

- Obter proventos ou qualquer outra vantagem resultante de atividades ilegais realizadas pelas organizações terroristas que foram financiadas. As outras vantagens podem consistir na proteção do negócio, em países em que tais organizações são muito influentes;

- Disfarçar a origem ilegal de proventos da infração.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de infração, 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 (isso é, 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 (por exemplo, FATF).

Principais padrões de conduta
As SNI devem condenar o uso de seus recursos para o financiamento ou execução de qualquer atividade voltada ao atingimento de objetivos associados com o financiamento do terrorismo, bem como qualquer utilização indevida de instrumentos e/ou da companhia.

De forma mais generalizada, devem condenar qualquer possível conduta voltada, ainda que indiretamente, a facilitar delitos, como recebimento, lavagem e utilização de dinheiro, bens ou qualquer outra utilidade de origem ilegal. Nesse sentido, estão comprometidas a implementar todas as atividades de controle preventivas e subsequentes necessárias para o atingimento de tal objetivo, regulando, ainda, as relações com Terceiros por meio de disposições contratuais que exijam a observância das leis aplicáveis relativas ao assunto.

Fica especificamente proibido:

a. Utilizar pagamento em branco ou dinheiro para qualquer operação de cobrança, pagamento, transferência de fundos, etc.;

b. Fazer ou receber pagamentos em contas bancárias anônimas ou localizadas em paraísos fiscais;

c. Emitir ou receber notas fiscais ou documentos de quitação em relação a operações não existentes.

Visando implementar os padrões de comportamento descritos acima, a SNI deve:

d. Realizar controles analíticos dos fluxos de caixa;

e. Verificar a validade dos pagamentos, controlando se o beneficiário final é efetivamente a contraparte envolvida na operação;

f. Realizar controles procedimentais, em especial no que tange a possíveis operações ocorridas fora dos processos normais da companhia;

g. Reter evidências de todas as operações realizadas;

h. Assegurar a rastreabilidade de cada operação financeira, bem como do contrato ou de qualquer outro investimento ou projeto de negócios;

i. Verificar a consistência econômica de tais operações e investimentos;

j. Sempre verificar a lista internacional relativa a terrorismo e aos paraísos fiscais.

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 alguém.

No entanto, para fins deste EGCP, os crimes contra pessoas referem-se principalmente àqueles que podem ocorrer com maior probabilidade na gestão de uma companhia, como os relativos a práticas de trabalho forçado, consistindo principalmente em coagir os empregados a trabalhar com o uso de violência ou intimidação ou por outros meios, como a retenção de documentos de identidade.

Pode ocorrer por diversas razões, incluindo, mas não se limitando a:

— Empregar mão de obra com despesas mínimas;

— Empregar mão de obra totalmente subserviente, para qual nenhum pedido seria recusado.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de crime, as seguintes áreas devem ser monitoradas:

— Celebração de contratos com Terceiros que utilizam profissionais não qualificados e/ou que operam em países em que direitos individuais não são totalmente protegidos pelas leis internacionais ou locais.

Principais padrões de conduta
As SNI devem:

a. Selecionar Terceiros externos (parceiros, fornecedores) – especialmente, aqueles que prestam serviços não técnicos – apenas após terem verificado de forma cuidadosa a sua confiabilidade;

b. Assinar documentação contratual adequada aos contratados externos, a qual exija que eles cumpram, e que seus subcontratados também cumpram, quaisquer leis locais e internacionais (como convenções da OIT acerca da idade mínima para trabalho e sobre as piores formas de trabalho infantil) relativas a trabalhos forçados, proteção do trabalho infantil e de mulheres, e observância das condições higiênicas e sanitárias;

c. Implementar e fazer cumprir quaisquer penalidades contratuais constantes no respectivo contrato em caso de violação por um contratado ou seus subcontratados, de quaisquer leis locais ou internacionais aplicáveis.

G. Crimes contra Saúde e Segurança

Crimes contra a saúde e a segurança são relacionados, principalmente, ao descumprimento de leis locais e normas trabalhistas a serem implementadas, 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 se limitando 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 os procedimentos e as políticas de precaução podem acelerar o processo de produção.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de crime, as seguintes áreas devem ser monitoradas:

i. Cumprimento de leis relativas à saúde e segurança.

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

Para esse fim, a SNI está comprometida a adotar todas as medidas necessárias, de forma a proteger a integridade física e moral dos trabalhadores.

Em especial, 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 os trabalhadores, na medida do possível e permitido pela evolução das melhores técnicas, seja avaliado 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 maneira adequada, por meio de medidas de segurança individuais e coletivas;

d. A informação e o treinamento dos trabalhadores sejam disseminados, atualizados e específicos 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 as inspeções, seja levada em consideração, de forma tempestiva e efetiva;

g. A organização da atividade de trabalho seja estruturada para proteger a integridade dos trabalhadores, de Terceiros e da comunidade em que a SNI opera.

Para conseguir o acima descrito, a SNI atribui recursos organizacionais, instrumentais e econômicos, tanto para assegurar o total cumprimento das disposições legais sobre a prevenção de acidentes industriais em vigor e para melhorar continuamente a saúde e a segurança dos trabalhadores e respectivas medidas preventivas.

Os Destinatários Corporativos, cada um de acordo com o seu papel dentro da organização, devem assegurar total respeito às disposições legais, aos procedimentos corporativos e quaisquer outros regulamentos internos voltados à 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.

Normalmente, eles afetam a qualidade do ar, da água e do solo, ameaçam a sobrevivência de espécies, podem causar desastres incontroláveis e apresentar ameaça à segurança de um enorme número de pessoas.

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

Esses tipos de conduta podem ocorrer em benefício da companhia por diversas razões, incluindo, mas não se limitando a:

— Reduzir custos, já que a adoção das medidas necessárias para proteção do meio ambiente, muitas vezes, resulta em despesas adicionais;

— Aumentar a produtividade, considerando que trabalhar sem levar em conta as questões ambientais pode acelerar o processo de produção.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de crime, as seguintes áreas devem ser monitoradas:

i. Observância das leis ambientais aplicáveis relativas ao desenho, à construção, gestão e manutenção de usinas e das infraestruturas relacionadas.

Principais padrões de conduta
Em seus negócios, a SNI deve seguir o princípio de proteção do meio ambiente.

Especialmente, ela deve:

a. Contribuir para a disseminação e o aumento da conscientização acerca da proteção do meio ambiente e administrar as atividades que lhe são confiadas, em conformidade com a legislação aplicável;

b. Promover o desenvolvimento científico e tecnológico voltado à preservação do meio ambiente e dos recursos por meio 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, adotar todos os instrumentos adequados de proteção e preservação e condenar qualquer forma de dano ao ecossistema.

Nos acordos celebrados com Terceiros em que possa surgir a responsabilidade da companhia nos termos da legislação ambiental, especialmente no que diz respeito à gestão e eliminação de resíduos, a empresa 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 infrações: uma em que o alvo é a rede ou um computador e outra em que os crimes são cometidos ou acelerados por um computador.

Para fins do EGCP, os crimes cibernéticos não incluem aqueles que podem ser facilitados por um delito informático, tais como fraude, roubo, chantagem, falsificação e assédio (por exemplo, *cyberbullying* ou *cyberstalking*).

Portanto, os crimes considerados pelo EGCP consistem, por exemplo, em: (i) intrusão não autorizada em uma rede protegida; (ii) introdução de vírus em um sistema de computadores; (iii) interceptação de dados de uma rede de computadores.

Eles podem ocorrer por diversas razões, incluindo, mas não se limitando 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.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse 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 das 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
As SNI devem avaliar a oportunidade de aplicar medidas técnicas, físicas e organizacionais adequadas, e cada Destinatário fica obrigado a não incorrer em:

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 da SNI;

f. Extração ilícita de dados da SNI;

g. Adulteração, furto ou destruição dos ativos informáticos da SNI (arquivos, dados e programas);

h. Uso de quaisquer falhas nas medidas de segurança do sistema de informações corporativas para acessar dados sem a autorização adequada;

i. Práticas de *spam*;

j. Acesso aos sistemas informáticos da SNI por meio de dispositivos externos (computador pessoal, periféricos, *hard drives* externos, etc.) e instalação de *softwares* e bases de dados sem a autorização prévia;

k. Instalação de *software* danoso (por exemplo, *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 (por exemplo, sistemas para identificar as credenciais, descriptografar arquivos, etc.).

A SNI, de forma a identificar condutas anormais, potenciais vulnerabilidades e deficiências nos sistemas corporativos, deve assegurar um monitoramento periódico das atividades desenvolvidas pelo pessoal da SNI no sistema corporativo de TI, de acordo com as leis locais aplicáveis.

Além disso, ela deverá periodicamente lembrar os Destinatários Corporativos de usar as ferramentas de TI em sua posse de maneira adequada, também por meio de treinamentos específicos quando necessário.

J. Crimes contra Direitos Autorais

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

Para fins do EGCP, os crimes contra direitos autorais referem-se principalmente àqueles delitos que podem ser contemplados mais facilmente na administração de uma companhia, tais como os relativos ao uso ilegal de *softwares* e bases de dados.

Esse tipo de crime pode ocorrer por diversas razões, incluindo, mas não se limitando a:

— Reduzir custos por meio do não pagamento de licenças de *softwares*.

Para mais detalhes, veja os exemplos fornecidos no Anexo 1.

Áreas a serem monitoradas
Em relação a esse tipo de crime, as seguintes áreas devem ser monitoradas:

i. Atividades da companhia desenvolvidas por Destinatários utilizando a intranet e qualquer outra ferramenta de TI fornecida pela SNI.

Principais padrões de conduta
Além dos principais padrões de conduta estabelecidos no parágrafo 8.2, as SNI deverão avaliar a oportunidade de adotar medidas técnicas, físicas e organizacionais de forma a evitar:

a. Qualquer uso ou disseminação ilegal para o público, por meio de redes baseadas em computadores ou via conexão de qualquer tipo, de trabalhos originais protegidos, ou de parte deles;

b. 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;

c. *Download* ilegal de qualquer *software* sem a assinatura da documentação contratual apropriada;

d. O *download* de *software* entre pares (*peer to peer*) ou qualquer outro *software* não ligado diretamente à atividade corporativa.

Caso a SNI tenha celebrado um contrato com contratados externos para a execução de atividades potencialmente afetadas pelo risco de violação de quaisquer direitos autorais, tal documento deve conter disposições que exijam o cumprimento das leis e dos regulamentos aplicáveis.

Anexo 1
Exemplos de condutas ilegais cometidas na ASM

A. CRIMES DE SUBORNO

Alguém dentro da SNI:

— Fornece presente a um funcionário público de forma a obter adjudicação de contrato em licitação;

— Dá dinheiro a um funcionário público durante inspeção em usina para convencê-lo a "fazer vista grossa" sobre algumas irregularidades;

— Promete contratar um empregado de uma concorrente em troca da obtenção de acesso a documentos secretos da empresa;

— Dá dinheiro a uma testemunha de forma a persuadi-la a dar falso testemunho em um julgamento em que a SNI esteja envolvida.

B. OUTROS CRIMES CONTRA AUTORIDADES PÚBLICAS

Alguém dentro da SNI:

— Durante o processo de apresentação de documentos ou dados para participar de uma licitação, presta informações não verídicas à entidade governamental de forma a assegurar o respectivo contrato;

— Presta uma declaração falsa sobre a situação financeira e comercial da SNI para obter dinheiro público;

— Abstém-se de cumprir contrato de outorga, utilizando indevidamente um financiamento recebido de entidade pública.

C. FRAUDE CONTÁBIL

Alguém dentro da SNI:

— Omite perdas significativas sofridas pela SNI nas demonstrações financeiras;

— Esconde a criação de caixa dois por meio da superestimação dos custos de serviços de consultoria recebidos pela SNI.

D. ABUSO DE MERCADO

Alguém dentro da SNI (presumindo que a SNI é a companhia aberta em relação aos primeiros dois exemplos):

— Divulga informações privilegiadas a um parente sobre uma aquisição futura, induzindo-o a comprar ações da companhia;

— Dissemina informações falsas sobre a situação financeira da SNI de forma a influenciar o preço das ações;

— Espalha informações falsas ou enganosas sobre empresa concorrente, prejudicando a sua reputação de mercado.

E. CRIMES DE FINANCIAMENTO DO TERRORISMO E LAVAGEM DE DINHEIRO

Alguém dentro da SNI:

— Recebe dinheiro de (ou transfere dinheiro para) companhia localizada em paraíso fiscal ou cuja conta bancária seja em um banco em paraíso fiscal, de forma a esconder a origem criminosa de tal dinheiro;

— Finge estar efetuando pagamentos a uma empresa por serviços de consultoria e transfere dinheiro a contas bancárias secretamente detidas por organização ilegal que financia o terrorismo;

— Utiliza caixa dois, cuja criação foi escondida por meio de manipulação das demonstrações financeiras da companhia, para financiar partidos políticos ligados a organizações terroristas.

F. CRIMES CONTRA A PESSOA

Alguém dentro da SNI:

— Tira vantagem da situação de necessidade física ou psicológica de um trabalhador, explorando-o;

— Compele indivíduos a trabalhar, utilizando ameaças, abuso de autoridade e/ou violência;

— Força imigrantes a trabalharem sob ameaça de denúncia às autoridades imigratórias.

Programa Global de *Compliance* relativo à responsabilidade corporativa | **Anexo 1 – Exemplos de condutas ilegais cometidas na ASM**

G. CRIMES CONTRA A SAÚDE E A SEGURANÇA

Alguém dentro da SNI, agindo em violação da legislação aplicável sobre saúde e segurança:

— Deixa de fornecer luvas e máscaras de proteção aos trabalhadores cujas atividades envolvam contato com materiais perigosos;

— Deixa de disponibilizar *kit* de primeiros socorros na área de trabalho;

— Deixa de fornecer os equipamentos de segurança necessários aos trabalhadores;

— Permite que os funcionários trabalhem com máquinas perigosas sem tê-los instruído sobre o seu uso seguro;

— Deixa de submeter os funcionários a exames periódicos por especialista médico para monitorar a sua saúde, avaliando se o trabalho que desempenham está prejudicando-os.

H. CRIMES AMBIENTAIS

Alguém dentro da SNI:

— Deixa de considerar a fauna local durante o planejamento da expansão de uma usina, danifica o *habitat* de espécime animal protegida, prejudicando a sua existência;

— Opera uma usina termoelétrica sem considerar os limites legais para emissão de gases, poluindo, assim, o ar na área adjacente;

— Deixa de executar a eliminação de resíduos da companhia adequadamente e, ao contrário, estabelece local ilegal para despejo dos resíduos;

— Permite que canos desaguem em rios, poluindo a água e prejudicando a fauna e flora aquáticas.

I. CRIMES CIBERNÉTICOS E CRIMES RELACIONADOS À VIOLAÇÃO DE DIREITOS AUTORAIS

Alguém dentro da SNI:

— Instala *software* copiado de forma ilegal em dispositivos de trabalho;

— Acessa o sistema de computadores de um concorrente por meio de *hacking*, a fim de roubar segredos comerciais;

— Introduz um vírus no sistema de computadores de um concorrente de forma a danificá-lo;

— Hackeia o sistema de computadores de um concorrente para ter sempre acesso a informações confidenciais sobre as suas atividades.

Programa Global de *Compliance* relativo
à responsabilidade corporativa