# PROGRAMA
## GLOBAL DE COMPLIANCE RELATIVO À RESPONSABILIDADE CRIMINAL CORPORATIVA

enel BRASIL

## INTRODUÇÃO

A Enel S.p.A.. ("**Enel**") é a holding de um grupo multinacional que atua em um setor empresarial complexo e altamente regulado e em diferentes ambientes econômicos, políticos, sociais e culturais. Nesse contexto, a integridade é entendida como um valor fundamental para a condução dos negócios. Isso exige que todo o pessoal do Grupo ENEL ("Grupo") atue com lealdade, correção, transparência e estrita conformidade com legislações e regulamentos nacionais e internacionais, bem como com padrões e diretrizes internacionais.

O "Programa Global de Compliance da Enel" (Enel Global Compliance Program ou "EGCP") foi criado como uma ferramenta para reforçar o compromisso da Enel com os mais altos padrões éticos, legais e profissionais, visando aprimorar e preservar a reputação do Grupo. Para tanto, estabelece uma série de medidas preventivas relacionadas à responsabilidade criminal corporativa.

Nos últimos anos, vem aumentando o número de países que instituíram regimes de responsabilidade criminal corporativa que permitem aos tribunais sancionar entidades corporativas por condutas criminosas praticadas por seus representantes, empregados ou terceiros agin- do em seu nome.

Em algumas jurisdições, as leis e regulamentações aplicáveis incentivam as empresas a adotarem estruturas de governança corporativa e sistemas de prevenção de riscos, com o objetivo de impedir que administradores, executivos, empregados, consultores e contratados ex- ternos cometam crimes, prevendo ainda isenção ou mitigação das penalidades em caso de adoção de medidas preventivas adequadas.

O EGCP, inspirado nas regulamentações internacionais mais relevantes, estabelece normas gerais de conduta aplicáveis a empregados, diretores e demais membros dos órgãos de administração e controle ("Destinatários Corporativos"), bem como consultores ou outros contratados e, em geral, terceiros ("Terceiros" ou "Outros Destinatários") - conjuntamente denominados "Destinatários" - que estejam empregados, nomeados ou que atuem em nome das subsidiárias não italianas ("Subsidiárias Não Italianas" ou "SNI"), inlcusive a Enel Brasil S.A. e suas subsidiárias.

O EGCP é aplicado 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.

Em caso de conflito entre o EGCP e outras normas internas ou técnicas, o EGCP prevalecerá. Nos casos em que as leis e regulamentos locais estabelecerem exigências específicas divergentes das disposições do EGCP, tais exigências prevalecerão.

## 1 MISSÃO

O EGCP representa uma oportunidade para reforçar uma prevenção proativa da responsabilidade criminal corporativa, por meio do aprimoramento do sistema de governança e con- trole interno, e foi concebido para apoiar a adoção de condutas adequadas e legais em todo o Grupo.

O EGCP identifica os principais padrões de comportamento esperados de todos os Destinatários Corporativos e, quando aplicável, de Outros Destinatários, a fim de:

**i.** fornecer à SNI um conjunto padrão de regras destinadas a prevenir a responsabilidade criminal corporativa em seus respectivos países; e
**ii.** integrar eventuais programas de compliance locais adotados pela SNI, de acordo com qualquer lei sobre responsabilidade criminal corporativa aplicável.

As regras previstas no EGCP são integradas:

**i.** pelas disposições do Código de Ética que representam os princípios éticos do Grupo ENEL, obrigatórios para todos os Destinatários;
**ii.** pelas disposições do Plano de Tolerância Zero à Corrupção adotado por todo o Grupo ENEL;
**iii.** pelas disposições de governança corporativa adotadas pela SNI, refletindo a legislação aplicável e as melhores práticas internacionais;
**iv.** pelo sistema de controle interno adotado pela SNI; e,
**v.** pelas disposições de quaisquer programas de compliance locais adotados por uma SNI para atender à legislação local sobre responsabilidade criminal corporativa, bem como quaisquer diretrizes, políticas ou documentos organizacionais internos relacionados.

## 2 ESTRUTURA

O EGCP contempla:

**a.** as modalidades de sua adoção pelas SNI e os processos de atualização correspondentes;
**b.** a divulgação do programa aos Destinatários e as atividades de treinamento;
**c.** o regime disciplinar aplicável em caso de violação de suas disposições;
**d.** normas gerais de controle;
**e.** as áreas de atividade a serem monitoradas em relação a determinados tipos de ondutas ilícitas (as "Áreas a Serem Monitoradas" ou "ASM"), conforme listadas na Seção 8 — que ão amplamente consideradas crimes e podem ser potencialmente cometidos por uma NI, cuja prevenção é prioritária para que a Enel conduza seus negócios com honestidade e integridade (os "Crimes");
**f.** os principais padrões de comportamento vinculados às "Áreas a Serem Monitoradas".

O EGCP é complementado pelo Anexo 1, que contém "Exemplos de Condutas Ilícitas nas ASM".

## 3 ADOÇÃO, IMPLEMENTAÇÃO, RESPONSABILIDADE E ALTERAÇÕES SUBSEQUENTES

O EGCP foi aprovado pelo Conselho de Administração da Enel e será submetido para aprovaçao dos Conselhos de Administração das SNI no Brasil. A aprovação do EGCP no Conselho de Administração da Enel Brasil S.A. implica na sua adoção e implementação nas SNI existentes no Brasil que não possuam Conselho de Administração.

O Conselho de Administração, ou órgão de administração de cada SNI, em conformidade com sua autonomia e independência:

**i.** adota as medidas adequadas para a implementação e monitoramento do EGCP, considerando a dimensão, a complexidade das atividades desenvolvidas, o sistema de controle interno e o perfil de risco específico da SNI e seu quadro regulatório, e
**ii.** é responsável pela implementação adequadas das "Áreas a Serem Monitoradas" e dos padrões fundamentais de comportamento, conforme estabelecido na seção 10.2 do EGCP, bem como dos controles determinados pelo Programa Global de Compliance da Enel.

O EGCP será aplicado pela SNI de acordo com a legislação aplicável, o tipo de negócio desenvolvido e as características específicas da estrutura organizacional.

O Conselho de Administração avalia e aprova propostas de emendas ou alterações ao Programa Global de Compliance da Enel.

Cada SNI deverá relatar alterações ou interpretações específicas realizadas de acordo com a legislação ou costumes locais. O Conselho de Administração ou órgão de administração da SNI deverá identificar a estrutura (indivíduo ou órgão) responsável por apoiar a implementação e mo- nitoramento do EGCP, bem como pela execução dos controles relacionados, em conformidade com os regulamentos aplicáveis.

## 4 DIVULGAÇÃO DO EGCP E ATIVIDADES DE TREINAMENTO

O EGCP estará disponível para download na intranet do Grupo Enel.

Serão oferecidas atividades específicas de treinamento a todo o pessoal (inclusive por meio de plataformas de e-learning), com o objetivo de garantir a divulgação e a correta compreensão do EGCP, das ASM e dos comportamentos relevantes para a prevenção dos Crimes. Essas atividades poderão ser organizadas também no âmbito de quaisquer programas de treinamento adotados pela SNI em conexão com a conformidade às legislações e programas de compliance locais.

## 5 COMUNICAÇÃO TERCEIROS

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

## 6 DENÚNCIAS DE DESTINATÁRIOS CORPORATIVOS OU DE TERCEIROS

Os beneficiários do EGCP (empregados, gerentes, diretores, demais membros dos órgãos de administração e terceiros) têm a obrigação de relatar qualquer possível má conduta, irregularidade ou não conformidade com o Programa Global de Compliance da Enel.

Em conformidade com a regulamentação vigente e sua "Política de Denúncias", a Enel estabeleceu um Canal de Denúncias dedicado, gerido pela Diretoria de Auditoria, que assegura a confidencialidade da identidade do denunciante, das pessoas mencionadas na denúncia, bem como do conteúdo e documentação relacionados. As comunicações podem ser realizadas:

**i.** por escrito, via web, por meio do sistema de denúncia online disponível no site do Grupo;
**ii.** oralmente, por telefone, contatando os números disponíveis na referida página web; ou
**iii.** mediante reunião presencial agendada a pedido do denunciante em prazo razoável por meio dos canais acima mencionados.

Conforme previsto no documento vigente, a Enel trata as denúncias dentro dos prazos regula- mentares, proíbe qualquer forma de retaliação e garante que não haverá atos retaliatórios em decorrência de uma denúncia.

A Enel aplica sanções disciplinares àqueles que: (i) violarem as medidas de proteção ao denunciante ou outras pessoas protegidas por lei; (ii) ocultarem ou tentarem ocultar uma denúncia; (iii) violarem as obrigações de confidencialidade previstas na legislação vigente sobre denúncias; (iv) forem responsáveis pela não criação ou pela gestão inadequada dos canais de denúncia, conforme requisitos estabelecidos na regulamentação vigente; (v) deixarem de verificar e analisar as denúncias; (vi) tomarem medidas retaliatórias contra o denunciante ou pessoas protegidas pela lei, em razão da mesma denúncia; bem como ao (vii) denunciante ou relator que, constatada sua responsabilidade criminal pelos crimes de difamação ou calúnia, inclusive por sentença de primeira instância, ou sua responsabilidade civil por dolo ou culpa grave.

## 7 SISTEMA DISCIPLINAR

Medidas disciplinares adequadas serão aplicadas pelas funções competentes da SNI em caso de violação de qualquer padrão de comportamento previsto no EGCP, de acordo com o sistema disciplinar vigente, normas aplicáveis ou programas de compliance locais e sem prejuízo dos direitos concedidos aos empregados, conforme disposto na legislação local (por exemplo, direito à defesa e princípio do contraditório).

As medidas disciplinares serão aplicadas independentemente de eventual processo criminal conduzido pela autoridade competente.

A documentação contratual deverá prever sanções adequadas, incluindo, mas não se limitando à rescisão contratual, conforme a legislação aplicável, em caso de violação de qualquer disposição do EGCP por Terceiros.

## 8 CRIMES

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

**A.** Crimes de Suborno
**B.** Outros Crimes contra Autoridades Públicas
**C.** Fraudes Contábeis
**D.** Abuso de Mercado
**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 relacionados à violação de Direitos Autorais
**K.** Crimes Fiscais

A Seção 10.2 do EGCP identifica as áreas de atividade a serem monitoradas pelas SNI e os padrões de comportamento aplicáveis.

A lista do parágrafo 10.2 não exime as SNI de realizarem suas próprias avaliações de risco e da definição de padrões principais de comportamento, caso seja considerado necessário.

Portanto, a SNI poderá identificar:

**i.** as atividades comerciais que possam implicar risco específico de ocorrência de crime, por meio da análise dos processos comerciais e das possíveis formas em que o crime pode ocorrer;

**ii.** padrões adicionais de comportamento que todos os Destinatários Corporativos e quando expressamente indicado – Outros Destinatários devem observar para: absterem-se de qualquer conduta que configure qualquer dos Crimes acima descritos; e absterem-se de qualquer conduta que, embora não constitua diretamente um dos Crimes listados, possa vir a configurá-los.

## 9 SISTEMA DE CONTROLE DO EGCP

O EGCP prevê dois principais níveis de controle em relação às ASM:

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

## NORMAS GERAIS DE CONTROLE

A SNI deverá observar as seguintes normas gerais de controle:

**1)** **Segregação de funções**: a atribuição de papéis, tarefas e responsabilidades dentro da SNI deve respeitar a segregação de funções, segundo a qual nenhum indivíduo pode executar de forma autônoma um processo completo — ou seja, nenhum indivíduo pode ser responsável simultaneamente por executar, autorizar e posteriormente verificar uma ação. A segregação adequada pode ser garantida também por sistemas de TI que restrinjam determinadas transações a pessoas identificadas e autorizadas;

**2)** **Poder de assinatura e autorização**: devem existir regras formais para o exercício de poderes internos e de assinatura, as quais devem estar alinhadas às responsabilidades organizacionais e gerenciais atribuídas a cada representante legal da SNI.

3. **Transparência e rastreabilidade dos processos**: a identificação e rastreabilidade das fontes, informações e controles efetuados que suportam a formulação e implementação da decisão da SNI, bem como a gestão dos recursos financeiros devem ser sempre garantidas. Deve ser garantido o armazenamento adequado dos dados e informações relevantes, por meio de sistemas de informação e/ou suporte em papel.
4. **Gestão adequada das relações com Terceiros:**
   **(i)** *Due diligence* adequada de requisitos de integridade antes do estabelecimento de qualquer relacionamento. A extensão da *due diligence* (que pode incluir consultas a contatos comerciais, câmaras de comércio locais, associações empresariais ou pesquisas na internet e acompanhar quaisquer referências comerciais e demonstrações financeiras) deve ser proporcional ao risco real ou percebido de que o potencial parceiro, consultor ou fornecedor não atenda aos requisitos acima. Circunstâncias que podem ser consideradas sinais de alerta incluem, entre outras:
   - o Terceiro está constituído num país que, de acordo com índices internacionais, como o Índice de Percepção da Corrupção da Transparência Internacional, é conhecido pela corrupção generalizada, ou num país que é considerado um "país não cooperativo" de acordo com a lista restritiva do FATF (*Financial Action Task Force*) ou outra lista internacional preparada por instituições internacionais em relação à luta global contra o financiamento do terrorismo e a lavagem de dinheiro;
   - o Terceiro está ou esteve suspenso de participar de licitações ou celebrar contratos com empresas estatais/órgãos públicos/agências governamentais devido a investigações de conformidade realizadas pelas autoridades públicas;
   - o Terceiro já foi sujeito a processo criminal;
   - o Terceiro se recusa a seguir o programa de compliance adotado pela empresa e não possui nenhum código de conduta ou conjunto semelhante de regras;
   - o Terceiro possui relação familiar com um executivo de órgão governamental ou com um servidor público estrangeiro;
   - um servidor público é o proprietário, gerente administrativo ou acionista majoritário do Terceiro;
   - o endereço comercial do Terceiro é um escritório virtual;
   - o Terceiro possui um sócio ou beneficiário não divulgado.

**(ii)** verificações adicionais, caso, durante a fase de *due diligence*, surjam quaisquer "sinais de alerta";

**(iii)** monitoramento periódico durante o relacionamento para garantir que a contraparte continue atendendo aos requisitos aprovados pela SNI, e;

**(iv)** medidas apropriadas a serem aplicadas caso um Terceiro não cumpra esses requisitos, ou qualquer outro "sinal de alerta" surja durante o curso do relacionamento contratual, como:

- o Terceiro insiste em lidar com funcionários públicos por conta própria, não permitindo qualquer participação da empresa;
- o Terceiro solicita pagamentos antecipados incomuns;
- o Terceiro oferece enviar ou envia faturas inexatas ou faturas por serviços que não foram atribuídos ou não foram realizados;
- o Terceiro solicita que os pagamentos sejam efetuados em dinheiro ou instru- mento ao portador;
- o Terceiro solicita que os pagamentos sejam efetuados fora do seu país de origem, numa jurisdição que não tenha qualquer relação com as entidades envolvidas na transação ou com a operação em si;
- o Terceiro solicita que o pagamento seja efetuado a um intermediário ou a outra entidade ou que os pagamentos sejam efetuados a duas ou mais contas bancárias;
- o Terceiro solicita que os fundos sejam doados a uma instituição ou fundação sem fins lucrativos.

## 10 ÁREAS A SEREM MONITORADAS E PRINCIPAIS PADRÕES DE CONDUTA

### A. Crimes de Suborno

Este tipo de crime refere-se à oferta, doação, solicitação ou recebimento de dinheiro (ou qualquer outro benefício, ganho ou vantagem) com a finalidade ou intenção de influenciar o destinatário - que pode ser um indivíduo pertencente a empresa privada ou um funcionário público - para que este atue de forma favorável à parte que oferece o suborno.

Subornos geralmente consistem em presentes ou pagamentos em dinheiro, mas também podem incluir bens, privilégios, entretenimentos e favores, em troca de tratamento favorável. Exemplos desse tratamento incluem, entre outros:

- contratação do corruptor para um contrato relevante (seja com a administração pública ou empresa privada);
- adjudicação de uma licitação pública;
- falso depoimento favorável ao corruptor por uma testemunha em um julgamento; e,
- relatório leniente emitido por funcionário público.

Para mais detalhes, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

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

**(i)** negociação, execução e gestão de contratos relevantes com qualquer parte (autoridades públicas, empresas, associações, fundações, etc.);
**(ii)** participação em licitações públicas ou privadas;
**(iii)** gestão de relacionamentos – diferentes dos relacionamentos contratuais – com orga- nizações comunitárias e autoridades públicas (por exemplo, com referência a requisitos de saúde, segurança e meio ambiente, gestão de pessoal, pagamento de tributos);
**(iv)** gestão de litígios (ações judiciais, arbitragem, procedimentos extrajudiciais);
**(v)** seleção de parceiros, intermediários e consultores, e negociação, execução e gestão dos contratos relevantes;
**(vi)** gestão de caixa e recursos financeiros;
**(vii)** gestão de iniciativas sem fins lucrativos;
**(viii)** gestão de presentes, entretenimentos e despesas de hospitalidade;
**(ix)** reembolso de despesas incorridas por empregados;
**(x)** contratação de pessoal; e
**(xi)** definição de incentivos de remuneração (por exemplo, Gestão por Objetivos - MBOs) destinados a executivos da SNI.

**PRINCIPAIS PADRÕES DE CONDUTA**

Ao conduzir negócios com empresas privadas, administrações públicas, governos internacionais, nacionais, estaduais e locais (as "Autoridades Públicas"), a SNI e seus

representantes comprome- tem-se a agir com integridade e honestidade, cumprindo todas as leis e regulamentos aplicáveis.

Destinatários Corporativos e Terceiros (de acordo com os termos contratuais aplicáveis) estão expressamente proibidos de:

**a)** oferecer dinheiro ou conceder outras vantagens de qualquer tipo (promessas de emprego, etc.) a representantes de Autoridades Públicas, bem como a indivíduos pertencentes a uma empresa privada – ou a membros de suas famílias (coletivamente, os "Indivíduos Privados") – com os quais a SNI pretenda iniciar já possua um relacionamento comercial ou, no caso de Autoridades Públicas, qualquer outro relacionamento, incluindo a solicitação de fundos públicos, apresentação de qualquer autorização ou liberação pública, etc.

**b)** oferecer presentes, hospitalidades ou outros benefícios aos indivíduos listados no ponto a) acima, além do que é admitido de acordo com a prática corporativa padrão. Presentes, hospitalidades ou outros benefícios que não são admitidos incluem, mas não estão limitados a:

**(i)** viagens;

**(ii)** presentes ou entretenimento envolvendo partes com as quais uma SNI ou qualquer outra empresa pertencente ao Grupo Enel esteja atualmente envolvida em uma licitação, processo de licitação competitivo ou outros procedimentos públicos.

São permitidos exclusivamente presentes, hospitalidades ou outros benefícios considerados cortesia comercial.

Presentes e hospitalidades admitidos incluem, por exemplo:

**(i)** refeições ocasionais modestas;

**(ii)** presença ocasional em eventos esportivos locais, teatro ou outros eventos culturais; e

**(iii)** presentes de baixo valor nominal, como canetas, calendários ou outros pequenos itens promocionais.

Os presentes oferecidos - exceto aqueles de valor modesto - devem ser documentados para permitir as inspeções necessárias;

**c)** utilizar dinheiro em espécie como meio de pagamento fora dos casos permitidos pela
regulamentação (por exemplo, caixa pequeno);

**d)** incorrer em quaisquer despesas promocionais ou de patrocínio, a menos que as despesas tenham sido aprovadas, previamente, por escrito, pelo responsável competente;

**e)** fazer quaisquer contribuições para instituições sem fins lucrativos, projetos de serviço comunitário e associações profissionais, a menos que as despesas tenham sido aprovadas, previamente e 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 que não seja suficientemente justificado em relação ao tipo de tarefa a ser executada e às práticas locais vigentes.

As SNIs deverão avaliar a oportunidade de adotar medidas organizacionais adequadas para impedir que qualquer Destinatário realize qualquer uma das atividades descritas acima. Além disso, a SNI deverá avaliar a oportunidade de adotar procedimentos adequados para garantir que:

**h)** sejam fornecidas provas adequadas em relação a quaisquer relacionamentos relevantes com Autoridades Públicas (por exemplo, processos administrativos visando a obtenção de uma autorização, licença ou ato similar, *joint ventures* com entidades públicas, apresentação de pedido para obtenção de determinada liberação pública);

**i)** as relações com as Autoridades Públicas, quando envolverem questões relativas aos interesses da SNI, sejam geridas por, pelo menos, duas pessoas autorizadas;

**j)** qualquer procedimento de recrutamento seja realizado unicamente com base numa necessidade empresarial real e demonstrável, o processo de seleção envolva pelo menos dois cargos distintos e seja baseado em critérios de objetividade, competência e profissionalismo, visando evitar favoritismo ou nepotismo e conflito de interesse;

**k)** planos de incentivos dos executivos sejam adotados de forma a garantir que os objetivos neles definidos não conduzam a comportamentos abusivos e, em vez disso, estejam focados num resultado possível, determinado, mensurável e relacionado com o tempo necessário para atingi-los;

**l)** em relação ao planejamento de projetos, sejam definidos prazos realistas;

**m)** em relação ao reembolso de despesas, a documentação adequada, incluindo recibos originais que comprovem o pagamento das despesas ou a ocorrência do custo, deve ser apresentada ao departamento de contabilidade apropriado antes do pagamento, e o pa- gamento ou despesa subsequente (ou recebimento do mesmo) estar descrito de forma precisa e refletida nos registros contábeis da respectiva SNI.

### B. Outros crimes contra Autoridades Públicas

Esse tipo de crime diz respeito principalmente a fraudes contra entidades públicas e ocorre quando uma empresa utiliza artifícios ou esquemas ilícitos para fraudar uma entidade pública ou obter vantagem econômica por meio de declarações, promessas ou pretensões falsas ou fraudulentas.

Geralmente, esses crimes estão vinculados a financiamentos públicos e subsídios, e ocorrem quando uma empresa solicita financiamentos públicos ou subsídios para os quais não é elegível ou os utiliza indevidamente de forma diversa daquela prevista no respectivo acordo.

Esse tipo de crime pode ocorrer por diversos motivos, normalmente relacionados à obtenção de vantagens econômicas indevidas.

Para mais detalhes, consulte os exemplos no Anexo 1.

ÁREAS A SEREM MONITORADAS

Em relação a esses crimes, devem ser monitoradas as seguintes áreas:

**(xii)** participação em licitações e procedimentos públicos em geral;
**(xiii)** gestão de relacionamentos com Autoridades Públicas (por exemplo, no que se refere a requisitos de saúde, segurança, meio ambiente, gestão de pessoal e pagamento de tributos);
**(xiv)** solicitação de financiamentos públicos, subsídios, outorgas ou garantias concedidas por Autoridades Públicas;
**(xv)** gestão de financiamentos públicos, subsídios, outorgas ou garantias recebidas.

**PRINCIPAIS PADRÕES DE CONDUTA**

Além dos principais padrões de comportamento estabelecidos no parágrafo 10.2. A) acima, os Destinatários Corporativos e Terceiros (de acordo com os termos contratuais específicos), de- vem abster-se de:

**a)** apresentar documentos falsos ou adulterados, no todo ou em parte, durante a participação em licitações públicas;
**b)** induzir, por qualquer forma, Autoridades Públicas a realizarem avaliação incorreta duran- te a análise de pedidos de autorização, licença, liberação, concessão, etc.;
**c)** omitir informação necessária de maneira a direcionar favoravelmente para a SNI decisões das Autoridades Públicas em relação a quaisquer das circunstâncias descritas nos pontos a) e b) acima;
**d)** qualquer conduta que vise obter de Autoridade Pública qualquer tipo de outorga, financiamento, empréstimo facilitado ou outros desembolsos da mesma natureza, por meio de declarações e/ou documentos alterados ou falsificados, ou da omissão de infor- mações relevantes ou, de forma geral, por meio de artifício ou fraude, visando induzir em erro a instituição outorgante;
**e)** utilizar recursos recebidos de Autoridades Públicas, como fundos, contribuições ou empréstimos, para fins diversos daqueles para os quais foram concedidos.

Além disso, para implementar os padrões de conduta descritos acima; as SNIs deverão avaliar a oportunidade de adotar medidas organizacionais adequadas, a fim de assegurar que:

**f)** todas as declarações apresentadas a Autoridades Públicas nacionais ou internacionais com a finalidade de obter fundos, outorgas ou empréstimos contenham apenas informações verdadeiras e sejam assinadas por signatários autorizados e, quando da obtenção de tais fundos, outorgas ou empréstimos, sejam devidamente contabilizados;

**g)** existam controles adequados de segregação de funções, garantindo que as fases de solicitação, gestão e elaboração de relatórios relativos a procedimentos públicos para fins de obtenção de fundos, outorgas ou empréstimos sejam geridos por diferentes Destina- tários Corporativos dentro da organização;

**h)** as atividades de coleta e análise das informações necessárias à elaboração do relatório sejam realizadas com o apoio das funções competentes;

**i)** a documentação e os relatórios subsequentes a serem apresentados em relação à solicitação de subsídios, outorgas, empréstimos e garantias sejam aprovados pelos níveis hierárquicos adequados.

### C. Fraudes Contábeis

A fraude contábil é um tipo de crime que consiste, principalmente, na manipulação intencional das demonstrações financeiras para criar uma representação falsa da saúde financeira de uma empresa perante investidores, credores, acionistas e demais partes interessadas.

Fraudes contábeis podem ocorrer por vários motivos, incluindo, mas não se limitando a:

**i.** continuar a obter financiamento de um banco (para este efeito, pode-se alterar a demonstração financeira de modo a criar uma representação da saúde financeira);
**ii.** relatar lucros irrealistas ou ocultar perdas;
**iii.** ocultar circunstâncias que possam afetar negativamente a empresa;
**iv.** causar inflação do preço das ações;
**v.** disfarçar a criação de caixa dois;
**vi.** encobrir condutas impróprias (tais como furtos praticados pela administração da empresa);
**vii.** omitir fatos relevantes que possam induzir a erro qualquer parte interessada (tais como partes interessadas, credores, autoridades da bolsa de valores, etc.).

Para mais detalhes, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

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

**(i)** elaboração de documentos a serem divulgados aos acionistas ou ao 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 documen- tos sejam diferentes dos documentos contábeis periódicos;
**(ii)** gestão de relacionamentos com os auditores externos e órgãos de supervisão.

**PRINCIPAIS PADRÕES DE CONDUTA**

As SNIs devem avaliar a implementação de medidas adequadas, e os responsáveis pela manutenção dos livros, registros e contas devem atuar de forma a garantir que:

**a)** os dados e informações utilizados na elaboração dos relatórios financeiros sejam precisos e rigorosamente verificados;
**b)** todos os itens do balanço, cuja determinação e quantificação impliquem avaliações di- scricionárias, sejam objetivos e apoiados por documentação apropriada;
**c)** as transações sejam executadas de acordo com as autorizações gerais ou específicas da administração;
**d)** as faturas e demais documentos relevantes relacionados às transações sejam devidamente verificados, registrados e armazenados;
**e)** as transações 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 quaisquer outros critérios aplicáveis a tais demonstrações;
**f)** o acesso aos registros de tais transações seja permitido somente de acordo com autorizações gerais ou específicas da administração.

Além disso, para garantir que informações completas e justas sejam fornecidas ao mercado, as SNIs ficam proibidas de realizar qualquer conduta que impeça e, de qualquer maneira, obstrua as atividades de verificação e auditoria dos auditores externos por meio da ocultação de documen- tação ou do uso de outros meios fraudulentos.

Por fim, as SNIs devem efetuar todas as comunicações a qualquer autoridade financeira pública (conforme previsto pela legislação local aplicável) de maneira correta, completa, adequada e célere, não as impedindo, de forma alguma, de desempenhar suas funções, mesmo no contexto de uma inspeção (por exemplo, oposição expressa, recusa injustificada, conduta obstrutiva ou falha em cooperar).

**D. Abuso de Mercado**

Esta categoria de crimes refere-se a três condutas principais: (1) comprar ou vender instrumen- tos 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 preços de instrumentos financeiros por meio da divulgação de informações sabidamente fal- sas ou enganosas para influenciar o preço de um instrumento financeiro; (3) executar ordens
de compra e venda que forneçam ou visem (i) fornecer indicações falsas ou enganosas quanto à oferta, demanda ou preço de instrumentos financeiros, (ii) fixar o preço de mercado de um ou mais instrumentos financeiros em um nível anômalo ou artificial.

Esses tipos de condutas podem ocorrer em benefício de uma empresa por vários motivos, inclu- indo, mas não se limitando a:

- deflacionar o preço das ações de uma empresa-alvo antes de uma aquisição;
- enfraquecer a reputação de uma empresa concorrente;
- alterar o preço de um determinado instrumento financeiro na carteira antes de realizar
  qualquer negociação relacionada a ele.

Para mais detalhes, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

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

**(xvi)** 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;

**(xvii)** gestão de Informações Privilegiadas relacionadas às companhias abertas do Grupo e aos
respectivos instrumentos financeiros (por exemplo, novos produtos/serviços e merca- dos, dados contábeis do período, dados de previsão e metas quantitativas relativas ao desempenho corporativo, fusões/cisões e, especialmente, novos negócios significativos, ou seja, negociações e/ou acordos relativos à aquisição e/ou venda de ativos relevantes);

**(xviii)** gestão de Informações Privilegiadas relacionadas a derivados de energia (por exemplo,
informação sobre indisponibilidade de usinas);

**(xix)** quaisquer tipos de informações relacionadas a instrumentos financeiros em portfólio.

**PRINCIPAIS PADRÕES DE CONDUTA**

É expressamente proibido a qualquer Destinatário:

**a)** utilizar Informações Privilegiadas para negociar, direta ou indiretamente, instrumentos financeiros para obter vantagem pessoal, ou para favorecer Terceiros, uma SNI ou qual- quer outra empresa do Grupo;

**b)** revelar Informações Privilegiadas a Terceiros, exceto quando exigido por lei, outras disposições regulatórias ou contratos específicos em que as contrapartes estejam obrigadas a utilizar as informações apenas para a finalidade originalmente pretendida e a manter a confidencialidade sobre elas;

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

Além disso, cada Destinatário é expressamente proibido de:

**d)** difundir informações falsas ou enganosas por meio da mídia (seja sobre a própria empresa ou sobre quaisquer outras empresas), 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 transações já planejadas pela pessoa que divulga tais informações;

**e)** realizar quaisquer transações sobre um instrumento financeiro (por exemplo, venda ou compra) em violação às normas de abuso de mercado.

## E. Fincanciamento ao 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 dos indivíduos ou entidades envolvidos no financiamento do terrorismo é ocultar tanto o financiamento quanto a natureza das atividades financiadas.
Lavagem de dinheiro é o processo pelo qual os proventos de uma atividade criminosa são disfarçados para ocultar sua origem ilícita. Mais precisamente, pode abranger três condutas alternativas diferentes: (i) a conversão ou transferência de fundos, sabendo que são produtos de crime, (ii) a ocultação ou disfarce da verdadeira natureza, origem, localização, disposição, movi- mentação ou propriedade ou direitos relativos à propriedade, sabendo que são proventos de um crime; e (iii) a aquisição, posse ou uso de propriedade, sabendo, no momento

do recebimento, que tal propriedade é produto de um crime. Quando os proventos de um crime são criados pela mesma pessoa que está ocultando sua origem ilícita, tal conduta é punida em certos países como autolavagem de dinheiro.

A lavagem de dinheiro e o financiamento do terrorismo, muitas vezes, apresentam característic- as operacionais semelhantes, principalmente relacionadas à ocultação. Os indivíduos que lavam dinheiro remetem fundos ilícitos por meio de canais legais para ocultar suas origens criminosas, enquanto aqueles que financiam o terrorismo transferem fundos que podem ser de origem legal ou ilícita de forma a ocultar sua origem e utilização final, que é o apoio ao terrorismo.

Esses tipos de condutas podem ocorrer em benefício de uma empresa por diversas razões, incluindo, mas não se limitando a:

- obter proventos ou outras vantagens resultantes de atividades ilegais realizadas pelas organizações terroristas que foram financiadas (as outras vantagens podem consistir na proteção do negócio, em países onde tais organizações são bastante influentes);
- disfarçar a origem ilícita de proventos criminosos.

Para mais detalhes, consulte os exemplos no Anexo 1.

## ÁREAS A SEREM MONITORADAS

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

- transações financeiras ou comerciais realizadas com pessoas físicas ou jurídicas - e pessoas jurídicas controladas direta ou indiretamente pelos sujeitos mencionados – que tenham residência ou sede em país que represente jurisdição de alto risco e não cooperativas (ou seja, com deficiências estratégicas em seus regimes de combate à lavagem de dinheiro e ao financiamento da proliferação do terrorismo), segundo avaliação de autoridades internacionais (ex.: FATF).

## PRINCIPAIS PADRÕES DE CONDUTA

A SNI rejeita veementemente o uso de seus recursos para financiar ou executar atividades relacionadas com financiamento ao terrorismo, bem como qualquer uso indevido de instrumentos financeiros ou operações que visem ocultar a origem dos fundos da empresa.

De forma generalizada, a SNI condenará qualquer possível conduta que vise, ainda que indiretamente, facilitar a prática de delitos como o recebimento, a lavagem e o uso de dinheiro, bens ou qualquer outra utilidade de origem ilícita. Neste sentido, a SNI se compromete a implementar todas as atividades de controle preventivas e subsequentes necessárias para atingir esse objetivo, regulando também as relações com Terceiros por meio de disposições contratuais que exijam a observância das leis aplicáveis relativas aos assunto.

É expressamente proibido:

**a)** utilizar pagamento em branco ou dinheiro para qualquer operação de cobrança, pagamento, transferência de fundos, etc.;
**b)** efetuar ou receber pagamentos em contas bancárias anônimas ou em contas bancárias localizadas em paraísos fiscais;
**c)** emitir ou receber notas fiscais ou documentos de quitação relativos a transações inexistentes.

Além disso, para implementar os padrões comportamentais descritos acima, a SNI deve:

**d)** realizar controles analíticos dos fluxos de caixa;
**e)** verificar a validade dos pagamentos, controlando se o seu beneficiário é realmente a contraparte envolvida na transação;
**f)** realizar controles procedimentais, em especial no que se refere a eventuais transações que ocorram fora dos processos normais da empresa;
**g)** reter evidências de todas as transações realizadas;
**h)** garantir a rastreabilidade de todas as operações financeiras, bem como de todos os contratos ou quaisquer outros investimentos ou projetos de negócios;
**i)** verificar a consistência econômica de tais operações e investimentos;
**j)** verificar a lista internacional relativa ao terrorismo e aos paraísos fiscais.

### F. Crimes contra pessoas

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

Entretanto, para os fins deste EGCP, crimes contra pessoas referem-se principalmente àqueles que podem ocorrer com maior probabilidade na gestão de uma empresa, como os relativos a práticas de trabalho forçado, consistindo principalmente em coagir empregados a trabalhar usando de violência ou intimidação, ou por outros meios, como retenção de documentos de identidade.

Este tipo de crime pode ocorrer por vários motivos, 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, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

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

**(xx)** celebrar contratos com fornecedores que utilizam pessoal não qualificado e/ou operam em países onde os direitos individuais não são totalmente protegidos pela legislação internacional ou local.

**PRINCIPAIS PADRÕES DE CONDUTA**

As SNIs devem:

**a)** selecionar Terceiros externos (por exemplo, parceiros, fornecedores) – especialmente aqueles que prestam serviços não técnicos – somente após verificar de forma cuidadosa a sua confiabilidade;

**b)** assinar a documentação contratual adequada com contratadas externas, exigindo que elas cumpram, e exigindo que suas subcontratadas também cumpram, quaisquer leis locais e internacionais aplicáveis (como Convenções da OIT sobre a idade mínima para o trabalho e sobre as piores formas de trabalho infantil) relativas a trabalho forçado, proteção do trabalho infantil e das mulheres e observância das condições higiênico-sanitárias; e

**c)** implementar e fazer cumprir quaisquer penalidades constantes no respectivo contrato em caso de violação por uma contratada ou qualquer uma das suas subcontratadas de quaisquer leis locais ou internacionais aplicáveis.

### G. Crimes contra a saúde e segurança

Os crimes contra saúde e segurança estão relacionados principalmente ao descumprimento das legislações locais e das normas trabalhistas a serem cumpridas no ambiente de trabalho, a fim de evitar acidentes e doenças dos trabalhadores.

Esses tipos de condutas podem ocorrer em benefício de uma empresa por vários motivos, inclu- indo, mas não se limitando a:

**i.** reduzir custos, uma vez que a adoção das medidas necessárias implica, muitas vezes, em despesas adicionais para a empresa;
**ii.** aumentar a produtividade, visto que trabalhar sem considerar procedimentos e políticas de precaução pode acelerar o processo de produção.

Para mais detalhes, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

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

**(i)** cumprimento das leis relativas à saúde e segurança.

**PRINCIPAIS PADRÕES DE CONDUTA**

Não obstante a dimensão local da legislação relativa à saúde e segurança no trabalho, a SNI deve promover e reforçar uma forte cultura de proteção da segurança no local de trabalho, aumentan- do a conscientização sobre os riscos e responsabilidades de condutas individuais.

Para esse fim, sem prejuízo do cumprimento da legislação local aplicável em matéria de segurança e saúde no trabalho, a SNI está comprometida em adotar todas as medidas necessárias, para proteger a integridade física e moral dos seus trabalhadores.

A SNI deve garantir que:

**a)** o respeito às disposições legais que regulam a segurança e a saúde dos trabalhadores no local de trabalho seja uma prioridade;
**b)** os riscos para os trabalhadores, na medida do possível e permitido pela evolução das melhores técnicas, sejam avaliados com o objetivo de proteção, inclusive pela

escolha dos materiais e equipamentos mais adequados e seguros, para eliminar ou, quando isso não for possível, reduzir o risco na fonte;

**c)** a informação e a formação dos trabalhadores sejam amplas, atualizadas e específicas em relação à atividade desenvolvida;

**d)** os trabalhadores sejam ouvidos periodicamente sobre questões relativas à saúde e segurança no trabalho;

**e)** seja implementado um processo de vigilância para garantir a implementação adequada e eficaz das medidas preventivas. Qualquer não conformidade ou área de melhoria, detectada durante a atividade de trabalho ou durante as inspeções periódicas, seja levada em consideração de forma tempestiva e eficaz;

**f)** a organização da atividade laboral esteja estruturada de forma a proteger a integridade dos trabalhadores, de terceiros e da comunidade em que a SNI opera.

Para atingir o acima exposto, a SNI aloca recursos organizacionais, instrumentais e econômicos tanto para assegurar o pleno cumprimento das atuais disposições legais sobre prevenção de acidentes de trabalho quanto para melhorar continuamente a saúde e a segurança dos trabalhadores no local de trabalho e as respectivas medidas preventivas.

Os Destinatários Corporativos, cada um de acordo com o seu papel dentro da organização, devem assegurar pleno 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 compreendem diversas práticas ilícitas, incluindo o comércio ilegal de animais selvagens, crimes relacionados à gestão inadequada de recursos hídricos, comércio ilícito e de- scarte indevido de resíduos perigosos, e contrabando de substâncias que destroem a camada de ozônio.

Crimes ambientais geralmente afetam a qualidade do ar, da água e do solo, ameaçam a sobrevivência de espécies e podem causar desastres incontroláveis, e apresentar ameaça à segurança de um enrome número de pessoas.

Impulsionados por grandes ganhos financeiros e facilitados por um baixo risco de detecção e escassas taxas de condenação, redes e grupos criminosos organizados estão cada vez mais in- teressados em tais atividades ilícitas e, frequentemente, transnacionais.

Esses tipos de condutas podem ocorrer em benefício de uma empresa por vários motivos, inclu- indo, mas não se limitando a:

- reduzir custos, já que a adoção das medidas necessárias à salvaguarda do meio ambiente implica, muitas vezes, em despesas adicionais; e
- aumentar a produtividade, visto que trabalhar sem considerar as questões ambientais pode acelerar o processo de produção.

Para mais detalhes, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

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

**(xxi)** observância das leis ambientais aplicáveis em relação ao desenho, construção, gestão e manutenção e desativação/desmontagem de instalações, interconexões e infraestruturas de redes de distribuição; e

**(xxii)** cumprimento das leis ambientais aplicáveis em relação ao fornecimento de produtos e
serviços relacionados com energia, eficiência energética e mobilidade elétrica a clientes residenciais, pequenas/médias/grandes empresas, bem como à administração pública; desenho, teste e desenvolvimento de produtos de mobilidade elétrica e inovação.

**PRINCIPAIS PADRÕES DE CONDUTA**

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

Em particular, a SNI deve:

**a)** contribuir para a divulgação e conscientização sobre a proteção ambiental e gerir as atividades que lhe são confiadas, em conformidade com a legislação aplicável;

**b)** promover o desenvolvimento científico e tecnológico visando a proteção do meio ambiente e a salvaguarda dos recursos, por meio da adoção, nas operações, de sistemas avançados de proteção ambiental e de eficiência energética;

**c)** trabalhar para atender às expectativas de seus clientes/partes interessadas em relação às questões ambientais e utilizar todos os instrumentos adequados para a proteção e preservação e condenar qualquer forma de dano ou prejuízo ao ecossistema.

Nos contratos firmados com Terceiros em que possa surgir a responsabilidade da empresa nos

termos da legislação ambiental, especialmente no que diz respeito à gestão e destinação de resíduos, a empresa deverá incluir disposições que imponham a tais Terceiros o cumprimento das leis aplicáveis e prevejam sanções contratuais em caso de violação.

### I. Crimes cibernéticos

Crimes cibernéticos envolvem infrações penais relacionadas a dois tipos principais: (i) aquelas cujo alvo são redes ou computadores; e (ii) aquelas executadas ou aceleradas por meio de computadores.

Para os fins do EGCP, não são considerados crimes cibernéticos aqueles facilitados por meio de crimes informáticos, como fraude, roubo, chantagem, falsificação ou assédio (ex.: cyberbullying ou perseguição cibernética).

Assim, os Crimes cibernéticos considerados pelo EGCP consistem, por exemplo, em: (i) intrusão não autorizada numa rede protegida; (ii) introdução de vírus num sistema de computadores; (iii) interceptação de dados de uma rede de computadores.

Os crimes cibernéticos podem ocorrer por vários motivos, incluindo, mas não se limitando a:
roubar o segredo comercial de um concorrente;

- colocar em risco ou danificar o sistema de computador de um concorrente;
- obter informações confidenciais acerca das estratégias de mercado de um concorrente.

Para mais detalhes, consulte os exemplos no Anexo 1.

## ÁREAS A SEREM MONITORADAS

Devem ser monitoradas:

**(i)** atividades da empresa realizadas pelos Destinatários utilizando recursos digitais em ambientes de TI e TO (Tecnologia Operacional) (por exemplo, Intranet, Internet, sistema de e-mail, aplicações empresariais, áreas de colaboração e compartilhamento de dados corporativos, mídias sociais, ferramentas de mensagens instantâneas);

**(ii)** gestão e proteção de dispositivos da empresa (por exemplo, estações de trabalho, smartphones, dispositivos removíveis) e infraestruturas (por exemplo, servidor, switch, roteador, firewall, armazenamento);

**(iii)** planejamento das medidas a serem adotadas para evitar riscos de perda de confidencia- lidade, integridade e disponibilidade de dados e informações; e

**(iv)** gestão de perfis dos administradores dos sistemas.

**PRINCIPAIS PADRÕES DE CONDUTA**

As SNIs devem avaliar a oportunidade de aplicar medidas técnicas, físicas e organizacionais adequadas para evitar e cada Destinatário é obrigado a não incorrer, por exemplo, em:

**a)** compartilhamento de credenciais e/ou uso indevido de credenciais pessoais para acessar dispositivos, sistemas ou infraestruturas de TI/TO;

**b)** o acesso ilícito de Terceiros aos sistemas ou infraestruturas de TI/TO;

**c)** a divulgação e compartilhamento não autorizados de informações e dados comerciais fora da empresa;

**d)** o acesso, extração e modificação não autorizados de informações e dados;

**e)** o uso de dispositivos pessoais ou não autorizados para transmitir ou armazenar informações ou dados da empresa;

**f)** o compartilhamento de dispositivos da empresa com outras pessoas;

**g)** a adulteração ou alteração das configurações dos dispositivos ou infraestruturas da em- presa;

**h)** a adulteração dos sistemas da empresa, roubo ou destruição de arquivos, dados e progra- mas;

**i)** o acesso aos sistemas de informação corporativos sem a devida autorização;

**j)** práticas de *spam*;

**k)** o acesso com dispositivos externos (computador pessoal, periféricos, discos rígidos exter- nos, etc.) aos sistemas ou infraestruturas da empresa e instalação de software e bases de dados sem autorização prévia;

**l)** a instalação de *softwares* nocivos (por exemplo, *worms* e vírus) em sistemas ou infraestruturas de TI e TO; e,

**m)** o uso de *softwares* e/ou *hardwares* não autorizados que possam ser usados para avaliar ou comprometer a segurança de dispositivos, sistemas e infraestruturas da empresa (por exem- plo, sistemas para identificar credenciais, descriptografar arquivos criptografados, etc.).

A SNI, de forma a identificar condutas anormais, potenciais vulnerabilidades e deficiências em sistemas e dispositivos corporativos, deverá garantir um monitoramento periódico das atividа- des realizadas pelo seu pessoal no sistema de TI corporativo, em conformidade com a legislação local aplicável.

Além disso, a SNI deve lembrar periodicamente os Destinatários Corporativos de usar os dispositivos, sistemas e infraestruturas da empresa em sua posse de forma adequada, também por meio de sessões de treinamento específicas, quando necessário.

**J. Crimes relacionados à violação de Direitos Autorais**

A violação de direitos autorais em ambiente corporativo consiste no uso, reprodução, distribu- ição ou adaptação não autorizados de obras protegidas pela legislação de direitos autorais, tais como softwares, bancos de dados, vídeos, imagens, obras literárias e musicais.

Para os fins deste EGCP, os crimes relacionados à violação de direitos autorais referem-se principalmente às infrações mais prováveis no contexto empresarial, como o uso ilícito de bancos de dados, *software* e a reprodução ou distribuição não autorizada de materiais pro- tegidos.

Esse tipo de crime pode ocorrer por diversos motivos, incluindo, mas não se limitando a:

**a)** falta de conscientização: os colaboradores podem inadvertidamente infringir direitos au- torais de terceiros devido ao treinamento insuficiente sobre as leis aplicáveis e as políticas da empresa;

**b)** pressão competitiva: em um mercado altamente competitivo a SNI pode cair no uso não autorizado de obras protegidas por direitos autorais para obter vantagem na redução dos custos de desenvolvimento;

**c)** intenção maliciosa: os colaboradores podem se envolver deliberadamente em violação de direitos autorais para prejudicar um concorrente da

SNI. Para mais detalhes, consulte os exemplos no Anexo 1.

**ÁREAS A SEREM MONITORADAS**

Em relação a este tipo de crime, é necessário monitorar a ocorrência dos seguintes comportamentos ou eventos:

- uso ou divulgação não autorizados de obras protegidas por direitos autorais, materiais de pesquisa ou conteúdo de titulariedade de terceiros;
- uso de imagens, vídeos ou músicas protegidos por direitos autorais em campanhas promocionais sem a devida autorização; uso não autorizado de *softwares*, pirataria

digital ou extração não autorizada de dados de bancos de dados; e,

- violação de direitos autorais decorrente de terceirização, *joint ventures* ou supervisão inadequada de acordos de licenciamento, direitos de distribuição de conteúdo ou gerenciamento de ativos digitais em acordos comerciais.

**PRINCIPAIS PADRÕES DE CONDUTA**

Além dos principais padrões de comportamento estabelecidos no parágrafo 10.2, seção I) acima, as SNIs deverão avaliar a oportunidade de adotar medidas técnicas, físicas e organizacionais adequadas para evitar:

1. qualquer uso ou divulgação ilegal ao público, por meio de redes de computadores ou por meio de conexão de qualquer tipo, de obra original protegida, ou parte dela;
2. utilização, distribuição, extração, venda ou arrendamento de conteúdo de uma base de dados violando o direito exclusivo de execução e autorização do titular dos direitos autorais;
3. *download* ilegal de qualquer *software* sem a assinatura da documentação contratual adequada;
4. o *download* de *softwares entre partes (peer-to-peer)* ou qualquer outro software não diretamente relacionado à atividade corporativa.

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

Tais medidas deverão obedecer aos seguintes pilares:

- respeitar os direitos autorais de terceiros: obter autorização adequada antes de usar ma- teriais protegidos por direitos autorais, incluindo imagens, vídeos, *software* e conteúdo escrito;
- respeitar as políticas internas e conduzir programas de treinamento: respeitar as políticas internas sobre uso, licenciamento e proteção de direitos autorais e compartilhá-las dentro da organização.

  Realizar programas de treinamento para alinhamento com as leis de direitos autorais em vigor; e monitorar internamente e relatar suspeitas de violações: incentivar os colaboradores a monitorar internamente e relatar qualquer suspeita de violação de direitos autorais ou uso não autorizado de conteúdo de titularidade de terceiros.

Além disso, as SNIs devem permanecer vigilantes no respeito a todas as formas de direitos de propriedade intelectual, incluindo marcas registradas, patentes, modelos de utilidade e segredos industrial,desenhos industriais, e indicações geográficas para garantir operações comerciais éticas e legais. Isso inclui conformidade com políticas internas para proteger todos os ativos intelectuais, promovendo uma cultura de conformidade e monitorando continua- mente o desenvolvimento de regulamentações de propriedade intelectual para se adaptar as práticas comerciais adequadamente. Ao fazer isso, as SNIs podem não apenas mitigar os riscos legais, mas também construir uma reputação de integridade e inovação em seus respectivos setores.

**K. Crimes Fiscais**

Este tipo de crime refere-se à conduta praticada pelo contribuinte em violação às disposições da legislação tributária, as quais têm por objetivo proteger os interesses da administração tributária no exercício de seus poderes de avaliação, controle e arrecadação de tributos.

Os crimes fiscais penalmente relevantes podem ser classificados, principalmente, em três cate- gorias: declarativos, documentais e relativos ao pagamento de tributos:

Os crimes declarativos são: i) declarações fraudulentas mediante a utilização de faturas ou outros documentos para operações inexistentes e/ou irregulares; ii) declarações fraudulentas por outros artifícios, isto é, efetuadas por meio de operações simuladas objetiva ou subjetivamente ou outros documentos falsos, diferentes dos primeiros; iii) outras formas fraudulentas suscetíveis de induzir em erro as autoridades fiscais;

- crimes documentais referem-se à emissão de faturas ou outros documentos para transações inexistentes e/ou irregulares; e
- os crimes relacionados com o pagamento de tributos referem-se à falta de pagamento de tributos retidos na fonte, ao crime próprio do agente retentor, à falta de pagamento de tributos, à restituição indevida e à sonegação fiscal fraudulenta.

Os crimes fiscais, em regra, são dolosos, isto é, requerem a intenção específica de sonegar tributos.

Ademais, poderá configurar-se como crime fiscal o descumprimento dos requisitos constantes dos incentivos fiscais e benefícios fiscais concedidos ao contribuinte conforme legislação respectiva.

**ÁREAS A SEREM MONITORADAS**

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

**(i)** gestão da tributação (incluindo a preparação de declarações fiscais e a gestão das obrigações relacionadas);
**(ii)** compilação, manutenção e armazenamento de registros contábeis relevantes para efeitos fiscais e outros documentos cujo armazenamento seja obrigatório;
**(iii)** faturamento corporativo;
**(iv)** contabilidade e faturamento *intercompany*;
**(v)** alienações de ativos e operações societárias;
**(vi)** gestão das relações com as autoridades fiscais; e
**(vii)** gestão de compensações.

**PRINCIPAIS PADRÕES DE CONDUTA**

Para garantir uma tributação justa, responsável e transparente, a SNI está comprometida em agir com integridade e honestidade e em adotar uma abordagem totalmente orientada para o cu- mprimento das leis tributárias aplicáveis nos países em que opera e em interpretar essas leis de forma responsável com o objetivo de mitigar o risco tributário e atender aos interesses de todas as partes interessadas.

Para implementar os padrões comportamentais descritos acima, as SNI são obrigadas a:

**a.** assegurar um comportamento correto e transparente, em total conformidade com a lei e os regulamentos, bem como com os procedimentos internos da empresa, na execução de todas as atividades destinadas, por um lado, à gestão da contabilidade, faturamento e manutenção dos respectivos registros contábeis para efeitos fiscais e, por outro lado, à gestão da tributação (incluindo a preparação de declarações fiscais e a gestão das obri- gações relacionadas);
**b.** verificar a confiabilidade dos formulários de declaração/pagamento do imposto de renda e do imposto sobre o valor agregado em relação aos registros contábeis, bem como a correção e a exatidão dos dados introduzidos nesses formulários;
**c.** verificar a correção e a precisão do cálculo dos impostos diretos e indiretos;
**d.** garantir a implementação de quaisquer novidades e alterações na legislação fiscal e, consequentemente, garantir a atualização contínua dos procedimentos e políticas internas;

**e.** verificar se os valores devidos a título de imposto de renda, imposto sobre o valor agregado e imposto retido na fonte certificados pela empresa como agente de retenção foram pagos corretamente;

**f.** verificar se os itens econômicos e financeiros relevantes para fins fiscais foram registrados em eventos comerciais que realmente ocorreram e foram devidamente documentados;

**g.** verificar o registro e a contabilização completos, precisos e oportunos de notas fiscais e outros documentos/fatos comerciais relevantes para fins fiscais;

**h.** assegurar a preservação/arquivamento dos registros e documentos contábeis cuja preservação seja obrigatória através de meios ou serviços digitais que garantam a sua disponibilidade e integridade;

**i.** verificar a completude e a exatidão dos dados informados na nota fiscal com base no que foi contratualmente acordado com o fornecedor ou cliente, bem como em relação aos serviços prestados;

**j.** garantir a mais alta integridade, transparência e correção substantiva e procedimental
nas transações com outras empresas do Grupo e que os serviços entre empresas sejam regulados contratualmente e prestados em condições de mercado;

**k.** definir os critérios, em conformidade com as disposições da respectiva regulamentação aplicável, para a determinação dos preços de transferência no contexto de transações *intercompany*;

**l.** definir as funções, deveres e responsabilidades no que diz respeito à verificação do cumprimento dos critérios adotados para a determinação dos preços de transferência;

**m.** garantir o envolvimento das respectivas áreas fiscais corporativas para a avaliação dos impactos fiscais e o cumprimento das regulamentações fiscais, em relação a operações corporativas extraordinárias;

**n.** verificar o cumprimento do procedimento de alienação e eliminação de ativos para o correto tratamento tributário;

**o.** assegurar transparência, equidade e cooperação nas relações com as autoridades fiscais, inclusive no caso de atividades de controle. Para consolidar a transparência perante as autoridades fiscais, promover a adesão aos regimes de compliance cooperativo para as entidades que atendem aos requisitos da regulamentação local, com o objetivo de fortalecer seus relacionamentos; e

**p.** verificar a conformidade com os requisitos regulatórios relativos a quaisquer compensações de impostos diretos e indiretos e a veracidade e precisão das certificações que comprovam os créditos fiscais.

## 10.3 DISPOSIÇÕES FINAIS

Para assegurar o cumprimento das disposições legais acima, a Enel implementa um sistema de políticas e procedimentos que atribui funções e responsabilidades específicas dentro da organização.

## ANEXO 1

## EXEMPLOS DE CONDUTAS LÍCITAS NA ASM

### A. Crimes de Suborno

Alguém dentro da SNI:

- fornece um presente a um funcionário público para vencer uma licitação;
- dar ou oferece dinheiro a um funcionário durante uma inspeção numa instalação para persuadi-lo a "fechar os olhos" a algumas irregularidades;
- promete contratar um colaborador de uma empresa concorrente em troca de obter acesso a documentos secretos da referida empresa concorrente;
- dar ou oferece dinheiro a uma testemunha para persuadi-la a fazer uma declaração falsa em um jul- gamento no qual a SNI está envolvida.

### B. Outros crimes contra autoridades públicas

Alguém dentro da SNI:

- durante o processo de submissão de documentos ou dados para participação em licitação, fornece informações falsas a um órgão governamental para garantir a respectiva adjudicação;

- fornece uma declaração falsa da situação financeira e empresarial da SNI para obterfinanciamento público;

- abstem-se de cumprir o contrato de financiamento, utilizando indevidamente um financia mento recebido por uma entidade pública.

### C. Fraudes contábeis

**Alguém dentro da SNI:**

- omite na demonstração financeira a comunicação de perdas relevantes sofridas pela SNI;
- disfarça a criação de caixa dois ao superestimar o custo dos serviços de consultoria recebidos pela SNI.

### D. Abuso de mercado

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

- divulga informações privilegiadas a um parente sobre uma aquisição futura, o induzindo a comprar ações da empresa;
- divulga informações falsas sobre a situação financeira da SNI para influenciar o preço de suas ações;
- espalha informações falsas ou enganosas sobre uma empresa concorrente para prejudicar sua reputação no mercado.

**E. Financiamento ao terrorismo e lavagem de dinheiro**

**Alguém dentro da SNI:**

- recebe dinheiro de (ou transfere dinheiro para) uma empresa localizada em um paraíso fiscal ou cuja conta bancária está em um banco em um paraíso fiscal para ocultar a origem criminosa desse dinheiro;
- finge pagar uma empresa por serviços de consultoria, transfere dinheiro para contas bancárias que são secretamente de titularidade de uma organização ilegal que financia ataques terroristas;
- utiliza fundos secretos, cuja criação foi disfarçada pela manipulação das demonstrações financeiras da empresa, para financiar partidos políticos ligados a organizações terroristas.

**F. Crimes contra pessoas**

Alguém dentro da SNI:

- aproveita-se da situação de necessidade física ou psicológica do empregado, explorando-o;
- obriga os indivíduos a trabalhar, usando ameaças, abuso de autoridade e/ou violência;
- obriga os indivíduos imigrantes a trabalhar sob ameaça de denúncia às autoridades de imigração.

**G. Crimes contra a saúde e segurança**

**Alguém dentro da SNI, agindo em desacordo com a legislação aplicável em matéria de saúde e segurança:**

- omite o fornecimento de Equipamentos de Proteção Individual (EPI) de acordo com a avaliação de risco;
- omite a implementação de medidas de emergência no local de trabalho (medidas organizacionais, de treinamento e técnicas);
- omite fornecer equipamentos e máquinas de segurança necessários aos trabalhadores;
- permite que os colaboradores trabalhem com máquinas sem que lhes tenham sido in- struídos sobre como trabalhar com segurança;
- omite a realização de exames periódicos dos colaboradores por médico especialista, nos termos da lei, para acompanhamento da saúde, avaliando se o trabalho que exercem lhes causa danos.

**H. Crimes ambientais**

**Alguém dentro da SNI:**

- abstém-se de considerar o impacto na biodiversidade ao planejar a expansão de uma instalação ou prejudica o habitat de espécies de animais protegidos, colocando assim em risco sua existência;
- opera uma estação termoelétrica sem respeitar os limites legais de emissão de gases, poluindo assim o ar da zona circundante;
- se abstém de realizar corretamente o descarte de resíduos da empresa e, pelo contrário, cria um local de descarte de resíduos ilícitos;

- causa poluição da água pelo uso inadequado do recurso ou pelo uso inadequado dos sistemas de tratamento de água;
- abstém-se de gerir adequadamente as emissões atmosféricas, não adotando sistemas adequados de prevenção e monitoramento, provocando poluição atmosférica.

**I. Crimes cibernéticos e crimes relacionados à violação de direitos autorais**

**Alguém dentro da SNI:**

- instala um *software* copiado ilegalmente em dispositivos de trabalho;
- entra no sistema de computador de uma empresa concorrente usando técnicas maliciosas de *hacking* para roubar informações e segredos comerciais e espalhar *malware* para danificá-lo.

**I. Crimes fiscais**

Alguém dentro da SNI:

- evade tributos:
  - utilizando faturas ou outros documentos para transações inexistentes e/ou irregulares, relatando na declaração de imposto de renda elementos passivos fictícios;
  - oculta ou destrói os documentos que devem ser conservados, de modo a impedir a reconstituição dos rendimentos ou do volume de negócios;
- emite ou libera notas fiscais ou outros documentos para transações inexistentes para permitir que terceiros soneguem tributos;
- não paga os tributos devidos, utilizando-se de créditos inexistentes ou indevidos como compensação.