Política de Controles Internos – POL 01

Abril – 2023 v6.0

Sumário

1. Controles Internos

Esta Política de Controles Internos ("Política"), foi elaborado pela **ENSO GESTÃO DE RECURSOS LTDA**. ("Enso") em conformidade as orientações da orientações da Comissão de Valores Mobiliários ("CVM"), principalmente, mas não se limitando, com o disposto no item 2.7 do Ofício-Circular/CVM/SIN/Nº 05/2014 e na Resolução da Comissão de Valores Mobiliários ("CVM") nº 21 de 21 de fevereiro de 2021, conforme alterada ("Resolução CVM nº 21") e se aplica a todos aqueles que possuam cargo, função, posição, relação societária, empregatícia, comercial, profissional, contratual ou de confiança ("Colaboradores" ou, individualmente "Colaborador") com a Enso, tanto na sua atuação interna quanto na comunicação com os diversos públicos.

A presente Política também foi elaborada observando as disposições do Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA de ART") e no Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação") ambos da Associação Brasileira das Entidades do Mercado de Capitais ("ANBIMA").

Na Enso, os controles e monitoramentos internos no que se refere ao cumprimento das regras e procedimentos internos e relativos à Política de Prevenção e Combate à Lavagem de Dinheiro e Anticorrupção é responsabilidade da área de Compliance, risco e PLD, liderada pelo Diretor de Compliance, Risco e PLD, abaixo identificado ("Área de Compliance").

A Área de Compliance tem como função assegurar o cumprimento integral das regras, políticas e procedimentos internos, assim como a adequação dos procedimentos internos às leis e regulamentações aplicáveis à Enso pela CVM, Banco Central do Brasil ("BACEN") e demais órgãos ou entidades de autorregulação, bem como é responsável por divulgar e treinar continuamente os Colaboradores para garantir a adequação, fortalecimento e o funcionamento do sistema de controles internos da Enso, e a constante avaliação e revisão dos procedimentos internos a fim de minimizar preventivamente eventuais riscos operacionais, potenciais situação de conflitos de interesse, falhas de segurança, o uso inadequado de autoridade e qualquer outro descumprimento ao Código de Ética e de Conduta e demais Políticas elaboradas pela Enso.

A Enso mantém versões atualizadas da presente Política em seu website (www.ensogp.com.br) juntamente com os seguintes documentos: (i) Formulário de Referência, conforme Anexo E da Resolução CVM nº 21; (ii) Política de Gestão de Risco; (iii) Política de Rateio e Divisão de Ordens; (iv) Política de Exercício de Direito de Voto; (v) Política de Investimentos Pessoais; e (vi) Código de Ética e Conduta; (vii) Política de PLDFT e KYC; (viii) Política de Análise do Perfil do Investidor (ix);

Política de Contratação de Terceiros; (x) Política de Seleção e Alocação de Ativos; e (xi) Política de Privacidade.

1.1 Sistema de Controles Internos

A fim de estabelecer um sistema de controles internos eficaz, a Enso utiliza-se de 03 (três) frentes de verificação e monitoramento, a saber:

- Primeira Frente: Gestão Operacional
- Segunda Frente: Área de Compliance
- Terceira Frente: Auditoria Interna

Embora complementares, as competências da Área de Compliance se distinguem daquelas atribuídas à Auditoria Interna, conforme expresso a seguir:

- Compliance: responsável por verificar a adesão dos Colaboradores da Enso aos sistemas de controles internos, leis, normas e regulamentos aplicáveis. Visa evitar a ocorrência de falhas durante as atividades da Enso.

- Auditoria Interna: responsável por atestar o cumprimento de normas e regulamentos externos, assim como políticas e procedimentos internos da Enso e indicar os riscos decorrentes de falhas eventualmente identificadas, assim como as soluções de remediação.

1.2 Primeira Frente: Gestão Operacional

O sistema de controles internos deve ser aplicado à todas as áreas da Enso. Neste sentido, cada área da Enso tem a responsabilidade primária de desenvolver e implementar seus próprios controles, contando sempre com a supervisão da Área de Compliance.

Assim, o sistema de controles internos da Enso tem início com o mapeamento dos processos adotados por cada área em suas atividades cotidianas, incluindo-se a definição de atribuições e responsabilidades de cada membro da área em questão.

Finalmente, cada área interna da Enso deverá avaliar a aplicação e eficiência de seus controles internos, cujas conclusões serão encaminhadas a Área de Compliance.

1.3 Segunda Frente: Área de Compliance

São atribuições da Área de Compliance:

- Orientar a implantação de estruturas de controles internos que contemplem registros bem documentados e identifiquem claramente as responsabilidades e atribuições dos envolvidos;
- Analisar os controles previstos na presente Política, propondo a criação de novos controles, assim como melhorias e correções aos já existentes, conforme necessário;
- Desenvolver as políticas internas Enso e disseminar suas regras e procedimentos entre os Colaboradores;
- Implementar e fiscalizar o cumprimento do sistema de controles internos da Enso;
- Estabelecer e monitorar, quando aplicável, a segregação de funções e áreas, orientando acerca das responsabilidades dos envolvidos e controle das atividades, com o objetivo de evitar eventuais conflitos de interesses e falhas nos controles internos;
- Planejar e executar as atividades e treinamentos a serem realizados ao longo do ano com o objetivo de mitigar os principais riscos aos quais a Enso está exposta em função de suas atividades e assegurar a conformidade da Enso com a legislação e regulamentação aplicáveis, assim como ao disposto nas políticas internas da Enso; e
- Atuar como interface da Enso junto ao BACEN, CVM, ANBIMA e demais órgãos reguladores ou autorreguladores, assim como perante auditorias externas.

Sem prejuízo das atribuições elencadas acima, competirá ao Diretor de Compliance, Risco e PLD analisar as avaliações periódicas realizadas pela Primeira Frente da Enso e propor as melhorias e correções que julgar necessárias.

Toda e qualquer melhoria e/ou correção proposta pela Área de Compliance deverá abordar: (i) natureza do evento; (ii) prazo para resolução; (iii) data do corrido; e (iv) classificação do risco, que poderá ser baixo, médio ou alto, de acordo com os critérios abaixo:

- **Baixo:** erros operacionais que resultem em infrações que não sejam consideradas graves e não desencadeiem aplicação de multas e nem causem perdas financeiras ou necessidade de comunicação ao mercado e/ou órgãos reguladores.
- **Médio:** erros operacionais que resultem em infrações que, embora não sejam consideradas graves, acarretem aplicação de multas e/ou perdas financeiras, sem que, no entanto, gerem necessidade de comunicação ao mercado e/ou órgãos reguladores.
- **Alta:** erros operacionais que sejam considerados graves, acarretem aplicação de multas e/ou perdas financeiras e gerem, ainda, necessidade de comunicação ao mercado e/ou órgãos reguladores.

Os resultados da análise das avaliações periódicas da Primeira Frente serão apresentados semestralmente pelo Diretor de Compliance, Risco e PLD, abaixo identificado, ao Comitê de Compliance, que discutirá as medidas a serem tomadas para correção dos riscos identificados.

- Monitoramento

Em linha com as disposições aplicáveis à Área de Compliance, mediante ocorrência de descumprimento, suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nesta Política ou aplicáveis às atividades da Enso, que cheguem ao conhecimento do Diretor de Compliance, Risco e PLD, de acordo com os procedimentos estabelecidos nesta Política, o Diretor de Compliance, Risco e PLD utilizará os registros e sistemas de monitoramento eletrônico referidos nesta Política para verificar a conduta dos Colaboradores envolvidos.

Todo conteúdo que está na rede será acessado pelo Diretor de Compliance, Risco e PLD, caso haja necessidade, inclusive arquivos pessoais salvos em cada computador serão acessados caso o Diretor de Compliance, Risco e PLD julgue necessário. Da mesma forma, mensagens de correio eletrônico de Colaboradores serão gravadas e, quando necessário, interceptadas e escutadas, sem que isto represente invasão da privacidade dos Colaboradores já que se trata de ferramentas de trabalho disponibilizadas pela Enso.

Adicionalmente, será realizado um monitoramento semestral, a cargo do Diretor de Compliance, Risco e PLD, sobre uma amostragem significativa dos Colaboradores, escolhida aleatoriamente pelo Diretor de Compliance, Risco e PLD, para que sejam verificados os arquivos eletrônicos, inclusive e-mails, com o objetivo de verificar possíveis situações de descumprimento às regras contidas na presente Política.

O Diretor de Compliance, Risco e PLD poderá utilizar as informações obtidas em tais sistemas para decidir sobre eventuais sanções a serem aplicadas aos Colaboradores envolvidos, nos termos desta Política. No entanto, a confidencialidade dessas informações é respeitada e seu conteúdo será disponibilizado ou divulgado somente nos termos e para os devidos fins legais ou em atendimento a determinações judiciais.

A Enso realizará inspeções com periodicidade semestral, a cargo do Diretor de Compliance, Risco e PLD, com base em sistemas de monitoramento eletrônico, independentemente da ocorrência de descumprimento ou suspeita ou indício de descumprimento de quaisquer das regras estabelecidas nesta Política ou aplicáveis às atividades da Enso, sendo tal inspeção realizada de forma aleatória.

Adicionalmente, o Diretor de Compliance, Risco e PLD deverá ainda verificar rotineiramente os

níveis de controles internos e Compliance junto a todas as áreas da Enso, com o objetivo de promover ações para esclarecer e regularizar eventuais desconformidades. Analisará também os controles previstos nesta Política, bem como em outras políticas da Enso, propondo a criação de novos controles e melhorias naqueles considerados deficientes, monitorando as respectivas correções.

Além dos procedimentos de supervisão periódica, o Diretor de Compliance, Risco e PLD poderá, quando julgar oportuno e necessário, realizar inspeções, nas ferramentas de trabalho, a qualquer momento sobre quaisquer Colaboradores.

1.4 Terceira Frente: Auditoria Interna

A Auditoria Interna constitui a última etapa dos sistemas de controles internos da Enso, e poderá ser executada com recursos da própria Enso ou por meio de firma externa contratada de acordo com a Política de Compras da Enso. Os resultados apurados serão enviados diretamente ao Diretor de Compliance, Risco e PLD que os compartilhará com os sócios e administradores da Enso, conforme indicados no contrato social, para que sejam tomadas as devidas providências.

O relatório de auditoria deverá conter, no mínimo:

- O escopo e abrangência da auditoria;
- Deficiências identificadas; e
- Recomendações de ações a serem executadas para correção das deficiências identificadas.

1.5. Aplicabilidade

A presente Política aplica-se a todos os Colaboradores que, por meio de suas relações com ou funções na Enso, possam ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

1.6. Ambiente Regulatório

Esta Política é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo de recebimento e compromisso constante do **Anexo I** a presente Política ("Termo de Recebimento e Compromisso"), estão aceitando expressamente as normas, princípios, conceitos e valores aqui estabelecidos.

Todos os Colaboradores devem se assegurar do perfeito entendimento das leis e normas aplicáveis à Enso bem como do completo conteúdo desta Política. Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da Enso foram apontadas no **Código de Ética e Conduta** da Enso.

1.7. Termo de Compromisso

Todo Colaborador, ao receber esta Política, firmará o Termo de Recebimento e Compromisso. Por meio desse documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos desta Política e com as normas, princípios, conceitos e valores aqui contidos; comprometendo-se a zelar pela aplicação das normas de Compliance e princípios nele expostos. Periodicamente, poderá ser requisitado aos Colaboradores que assinem novos Termos de Recebimento e Compromisso, reforçando o conhecimento e concordância com os termos desta Política.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos nesta Política ou das demais normas aplicáveis às atividades da Enso, deverá ser levado para apreciação do Diretor de Compliance, Risco e PLD, abaixo definido, de acordo com os procedimentos estabelecidos nesta Política. Competirá ao Diretor de Compliance, Risco e PLD aplicar as sanções decorrentes de tais desvios, nos termos desta Política, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar o Diretor de Compliance, Risco e PLD sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da Enso, bem como zelar pela reputação da Enso. Caso a violação ou suspeita de violação recaia sobre o próprio Diretor de Compliance, Risco e PLD, o Colaborador deverá informar diretamente aos demais administradores da Enso.

1.8. Governança da Área de Compliance

- Diretor de Compliance, Risco e PLD

A coordenação direta das atividades relacionadas a presente Política é uma atribuição do Sra. **Danielle Esteves Rodrigues Torres**, inscrito no CPF/ME sob o nº 222.281.068-01, na qualidade de diretor estatutário da Enso indicado como diretor responsável pelo cumprimento de regras, políticas, procedimentos e controles internos da Enso ("Diretor de Compliance, Risco e PLD"), nos termos da Resolução CVM nº 21.

- Comitê de Compliance e Risco

Ademais, a Enso possui também um Comitê de Compliance e Risco, que é composto pelo Diretor de Compliance, Risco e PLD, pelo Diretor de Gestão (abaixo definido) e pelos demais membros da Área de Compliance, que deverá e averiguar e debater possíveis falhas e oportunidades de aprimoramento nos controles internos da Enso, entre outros assuntos relacionados à área conforme descrito abaixo, além dos demais assuntos pertinentes à gestão de risco das carteiras, conforme Política de Gestão de Risco da Enso.

São atribuições do Comitê de Compliance e Risco da Enso relacionadas a esta Política:

- Analisar eventuais situações pelo Diretor de Compliance, Risco e PLD sobre as atividades e rotinas de Compliance;

- Revisar as metodologias e parâmetros de controle existentes; e

- Analisar eventuais casos de infringência das regras descritas nesta Política, nas demais políticas e manuais internos da Enso, das regras contidas na regulamentação em vigor, ou de outros eventos relevantes e definir sobre as sanções a serem aplicadas.

As reuniões do Comitê de Compliance e Risco serão realizadas mensalmente, e suas deliberações serão consignadas em atas e/ou registradas por e-mail.

1.9. Dúvidas ou ações contrárias aos princípios e normas da Política

A presente Política possibilita avaliar muitas situações de problemas éticos que podem eventualmente ocorrer no cotidiano da Enso, mas seria impossível detalhar todas as hipóteses. É natural, portanto, que surjam dúvidas ao enfrentar uma situação concreta que contrarie as normas de Compliance e princípios que orientam as ações da Enso.

Em caso de dúvida em relação a quaisquer das matérias constantes desta Política, também é imprescindível que se busque auxílio imediato junto ao Diretor de Compliance, Risco e PLD, para obtenção de orientação mais adequada.

Mesmo que haja apenas a suspeita de potencial situação de conflito ou ocorrência de uma ação que vá afetar os interesses da Enso, o Colaborador deverá seguir essa mesma orientação. Esta é a maneira mais transparente e objetiva para consolidar os valores da cultura empresarial da Enso e reforçar os seus princípios éticos.

Para os fins da presente Política, portanto, toda e qualquer solicitação que dependa de autorização, orientação ou esclarecimento expresso do Diretor de Compliance, Risco e PLD, bem como eventual

ocorrência, suspeita ou indício de prática por qualquer Colaborador que não esteja de acordo com as disposições da presente Política e das demais normas aplicáveis às atividades da Enso, deve ser dirigida pela pessoa que necessite da autorização, orientação ou esclarecimento ou que tome conhecimento da ocorrência ou suspeite ou possua indícios de práticas em desacordo com as regras aplicáveis, ao Diretor de Compliance, Risco e PLD, por meio de e-mail ou de maneira anônima via Canal de Denúncias, disponível no website da Enso (www.ensogp.com.br/compliance).

2. Política de Confidencialidade

2.1 Noções Gerais

As disposições do presente Capítulo se aplicam aos Colaboradores que, por meio de suas funções na Enso, possam ter ou vir a ter acesso a informações confidenciais, reservadas ou privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras.

Todos os Colaboradores deverão ler atentamente e entender o disposto nesta Política, bem como deverão firmar o termo de confidencialidade, conforme modelo constante no anexo a esta Política ("Termo de Confidencialidade").

Conforme disposto no Termo de Confidencialidade, nenhuma Informação Confidencial, conforme abaixo definido, deve, em qualquer hipótese, ser divulgada fora da Enso. Fica vedada qualquer divulgação, no âmbito pessoal ou profissional, que não esteja em acordo com as normas legais e de Compliance da Enso.

Quaisquer informações obtidas pelo vínculo de trabalho com a Enso são propriedade desta ou de seus clientes, conforme o caso. Desta maneira, os Colaboradores deverão presumir sempre que tais informações são Informações Confidenciais, conforme definido nesta Política.

Quando estiver em posse de Informações Confidenciais, os Colaboradores deverão ter o cuidado de assegurar sua confidencialidade e evitar divulgações não intencionais. Para tanto, a Enso recomenda evitar comentar e discutir quaisquer Informações Confidenciais em lugares públicos como restaurantes, aviões, elevadores, bem como adotar codinomes sempre que possível e manter documentos em lugares seguros quando estes não estiverem em uso.

É terminantemente proibido copiar, vender, usar ou distribuir quaisquer informações, políticas, documentos internos e/ou outras formas de propriedade intelectual da Enso ou de seus clientes, ainda que não confidenciais, sem o prévio e expresso consentimento por escrito da Enso.

Todo e qualquer material (incluindo, mas não se limitando a, planilhas, relatórios, documentos, etc.) desenvolvido por Colaboradores serão de propriedade desta, e não poderão, portanto, serem copiados, reproduzidos ou retirados de suas dependências, sob qualquer forma, sem o prévio e expresso consentimento por escrito da Enso.

Todos os Colaboradores devem ser orientados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias locais de fácil acesso, tendo sempre em mente o conceito de "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas, bem como garantir que o computador esteja sempre bloqueado quando o Colaborador estiver ausente de sua mesa para que nenhuma informação corra o risco de ser vazada.

2.2 Barreira de Informações

Quaisquer informações obtidas pela Enso e/ou seus Colaboradores serão classificadas conforme abaixo:

a) **Informação Pública:** é toda informação que pode ser acessada por usuários da Enso, clientes, fornecedores, prestadores de serviços e públicos geral.

b) **Informação Interna:** é toda informação que só pode ser acessada por Colaboradores da Enso. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

c) **Informação Confidencial:** é toda a informação que pode ser acessada por usuários da Enso e por parceiros da empresa. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

d) **Informação Restrita:** é toda a informação que pode ser acessada somente por usuários da organização explicitamente indicados pelo nome ou por área a que pertencem. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

As categorias de informações listadas acima serão disponibilizadas e acessadas aos Colaboradores exclusivamente de acordo com os termos expressos a seguir:

a) **Informação Pública:** poderão ser acessadas por todos e quaisquer Colaboradores, independentemente de seus cargos e atribuições.

b) **Informação Interna:** poderão ser acessadas apenas pelas áreas responsáveis pela determinada informação, a depender do caso concreto (ex: backoffice, administrativo, etc).

c) **Informação Confidencial:** da mesma forma poderão ser acessadas apenas pelas áreas e pessoas responsáveis que tenham demonstrada real necessidade da informação confidencial para realizar as atividades.

d) **Informação Restrita:** poderão ser acessadas apenas por aqueles que tenham extrema necessidade de tal informação para a realização das atividades internas.

Vale ressaltar que aqueles que tiverem acesso a determinadas informações, sendo internas, confidenciais e/ou restritas, existe um controle interno no drive da Enso que bloqueia e/ou dá acesso a determinadas e específicas informações a cada Colaborador de acordo com a necessidade do conhecimento de tal informação, havendo, dessa forma, um controle rígido e conhecido de quem obtém quais informações.

As Informações Internas, Informações Confidenciais e a Informação Restrita não podem ser divulgadas, em hipótese alguma, a terceiros não-Colaboradores ou a Colaboradores não autorizados.

Sem prejuízo da colaboração da Enso com as autoridades fiscalizadoras de suas atividades, a revelação de Informações Internas, Informação Confidencial ou Informação Restrita a autoridades governamentais ou em virtude de decisões judiciais, arbitrais ou administrativas, deverá ser prévia e tempestivamente informada ao Diretor de Compliance, Risco e PLD, para que esta decida sobre a forma mais adequada para tal revelação, após exaurirem todas as medidas jurídicas apropriadas para evitar a supramencionada revelação.

Em nenhuma hipótese as Informações Internas, Informações Confidenciais ou Informações Restritas poderão ser utilizadas para a prática de atos que configurem Insider Trading, Dicas ou Front-running.

<u>Insider Trading e “Dicas”</u>

Insider Trading significa a compra e venda de títulos ou valores mobiliários com base no uso de Informações Internas, Informações Confidenciais ou Informações Restritas, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo os Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, estranho às atividades da Enso, de Informações Internas, Informações Confidenciais ou Informações Restritas que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

Front-running

Front-running significa a prática que envolve aproveitar Informações Internas, Informações Confidenciais ou Informações Restritas para realizar ou concluir uma operação antes de outros.

O disposto nos itens acima deve ser analisado não só durante a vigência de seu relacionamento profissional com a Enso, mas também após o seu término.

Os Colaboradores deverão guardar sigilo sobre quaisquer Informações Internas, Informações Confidenciais ou Informações Restritas às qual tenham acesso, até sua divulgação ao mercado, bem como zelar para que subordinados e terceiros de sua confiança também o façam, respondendo pelos danos causados na hipótese de descumprimento.

Caso os Colaboradores tenham acesso, por qualquer meio, a Informações Internas, Informações Confidenciais ou Informações Restritas, deverão levar tal circunstância ao imediato conhecimento do Diretor de Compliance, Risco e PLD, indicando, além disso, a fonte da Informação Confidencial assim obtida. Tal dever de comunicação também será aplicável nos casos em que a Informações Internas, Informações Confidenciais ou Informações Restritas seja conhecida de forma acidental, em virtude de comentários casuais ou por negligência ou indiscrição das pessoas obrigadas a guardar segredo. Os Colaboradores que, desta forma, acessarem a Informações Internas, Informações Confidenciais ou Informações Restritas, deverão abster-se de fazer qualquer uso dela ou comunicá-la a terceiros, exceto quanto à comunicação ao Diretor de Compliance, Risco e PLD anteriormente mencionada.

É expressamente proibido valer-se das práticas descritas acima para obter, para si ou para outrem, vantagem indevida mediante negociação, em nome próprio ou de terceiros, de títulos e valores mobiliários, sujeitando-se o Colaborador às penalidades descritas nesta Política e na legislação aplicável, incluindo eventual demissão por justa causa.

3. Política de Segurança da Informação e Segurança Cibernética

3.1 Noções Gerais

A segurança da informação constitui uma proteção contra seu uso não autorizado, sua divulgação inadequada, alteração ou destruição, ainda que de forma não intencional.

Neste sentido, a função da presente Política de Segurança da Informação da Enso é proteger toda e qualquer informação obtida por esta, através de procedimentos específicos como, por exemplo: controles de acesso, segregações de funções, barreira de informações, criação de regras, políticas e procedimentos e, finalmente, capacitação e treinamento dos Colaboradores acerca de segurança da informação.

A presente Política de Segurança da Informação visa ainda garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para realização dos negócios da Enso. É dever de todos considerar as informações obtidas como sendo um ativo/bem da empresa, um dos recursos essenciais para a realização do negócio, que possui grande valor para a Enso e deve sempre ser tratadas de forma profissional.

Considerando o acima exposto, a Enso entende que uma Política de Segurança da Informação eficaz deverá compreender, sem prejuízo de outros, os seguintes aspectos:

- Os principais pontos de infraestrutura por onde circulam quaisquer informações, tais como telefonia, e-mails e internet em geral, devem possuir sistemas de back-up;
- Estabelecer controle de acesso à Informações Internas, Confidenciais e Restritas, bem como métodos para seu arquivamento seguro.
- Proibir expressamente a divulgação e/ou o compartilhamento indevido de informações privadas em fóruns de discussão online;
- Proibir expressamente o envio, armazenamento e manuseio de material que caracterize a divulgação, incentivo ou prática de atos ilícitos ou proibidos pelas Políticas Enso, ou que, de qualquer forma, possam danificar, inutilizar ou deteriorar os documentos e arquivos de qualquer tipo do usuário ou de terceiros.
- Nenhuma informação deve ser gravada nos diretórios locais dos computadores, mas sim na rede da Enso, em relação à qual deverá ser feito back-up em local seguro.
- Realização de testes periódicos de segurança para os sistemas de informação, em especial para os mantidos em meio eletrônico.

- Atribuição de senhas de caráter sigiloso, pessoal e intransferível para cada colaborador que necessite de acesso aos computadores da Enso, à rede corporativa e ao e-mail corporativo, sendo certo que tais senhas não poderão ser fornecidas a terceiros em nenhuma circunstância.

3.2 Dados Pessoais dos Colaboradores

A Enso se compromete a não acumular ou manter intencionalmente dados pessoais dos Colaboradores além daqueles relevantes para a condução do negócio. Todos os dados pessoais de Colaboradores são considerados dados pessoais.

Dados pessoais sob a responsabilidade da Enso não serão usados para fins diferentes daqueles para os quais foram coletados. Dados pessoais de Colaboradores não serão transferidos para terceiros, exceto quando exigido pelo negócio desde que os tais terceiros mantenham a confidencialidade de tais informações, e se comprometam a mantê-los confidenciais e com a autorização do Colaborador.

3.3 Programas Ilegais

É terminantemente proibido o uso de programas ilegais (piratas) na Enso. Os Colaboradores não podem, em hipótese alguma, instalar esse tipo de "software" (programas) nos equipamentos da empresa.

3.4 Permissões e Senhas (Acesso Escalonado ao Sistema)

Quando da necessidade de cadastramento de novo usuário para a utilização da "rede", sistemas ou equipamentos de informática da empresa, essa necessidade deverá ser levada à diretoria, e deve ser detalhado o tipo de rotinas e programas que o novo usuário terá direito de acesso e quais serão restritos.

A Enso mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores. As combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Enso necessária ao exercício de suas atividades.

A implantação destes controles é projetada para limitar a vulnerabilidade dos sistemas da Enso em caso de violação.

3.4.1 Senhas

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas somente pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros. As senhas deverão ser trocadas periodicamente, conforme aviso fornecido pelo responsável pela área de informática.

Cada computador deve ter sua senha pessoal e que deve ser atualizada periodicamente. A senha deve ser mantida apenas pelo profissional que utiliza a determinada máquina, não podendo compartilhá-la com ninguém, sendo de total responsabilidade do Colaborador o vazamento de informações, em caso de compartilhamento de senha.

3.4.2. Controle de Acesso

O acesso de pessoas estranhas à Enso a áreas restritas somente é permitido com a autorização expressa de Colaboradores autorizados pelos administradores da Enso.

Tendo em vista que a utilização de computadores, telefones, internet, e-mail e demais aparelhos se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos Colaboradores, a Enso monitora a utilização de tais meios.

3.4.3. Acesso Remoto

A Enso permite o acesso remoto pelos Colaboradores, de acordo com a seguinte regra: a todos os Colaboradores, conforme requisição por estes e autorização pelo Diretor de Compliance, Risco e PLD, no que se refere ao acesso ao e-mail e o acesso limitado a rede e diretórios específicos que permitam o desenvolvimento do trabalho remoto.

Ademais, os Colaboradores autorizados serão instruídos a (i) manter a utilização apenas em dispositivos que requeiram a inclusão de login e senha previamente ao acesso, (ii) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (iii) relatar ao Diretor de Compliance, Risco e PLD qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Enso e que ocorram durante o trabalho remoto, e (iv) não armazenar Informações Confidenciais ou sensíveis em dispositivos pessoais.

3.5 Cópia de Segurança do Sistema

Cópias de segurança são realizadas periodicamente e as informações desta cópia são acessíveis apenas pelos administradores da Enso, indicados em seu contrato social, em sua integralidade.

3.6 Admissão/Demissão de Funcionários Temporários/Estagiários

Toda contratação de funcionários temporários e/ou estagiários, admissão/demissão deve ser informada para que os mesmos possam ser cadastrados ou excluídos no sistema da empresa. Isto inclui o fornecimento de sua senha ("*password*") e registro do seu nome como usuário no sistema.

Em caso de desligamento de Colaborador, o desligamento a exclusão do acesso ao sistema deverá ser feito com urgência, de preferência, de forma imediata.

Nenhum Colaborador poderá ser contratado sem ter expressamente concordado com os requisitos de confidencialidade.

3.7 Propriedade Intelectual e Uso de Equipamentos e Sistemas

É de propriedade da Enso todos os "designs", criações ou procedimentos desenvolvidos por qualquer Colaborador durante o curso de seu vínculo empregatício com a Enso.

Cada Colaborador é responsável ainda por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

A utilização dos ativos e sistemas da Enso, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o Diretor de Compliance, Risco e PLD.

3.8. Identificação de Riscos (risk assessment)

No âmbito de suas atividades, a Enso identificou os seguintes principais riscos internos e externos que precisam de proteção:

- Dados e Informações: as Informações Confidenciais, incluindo informações a respeito de investidores, clientes, Colaboradores e da própria Enso, operações e ativos investidos pelas carteiras de valores miliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);

- Sistemas: informações sobre os sistemas utilizados pela Enso e as tecnologias desenvolvidas internamente e por terceiros, suas ameaças possíveis e sua vulnerabilidade;

- Processos e Controles: processos e controles internos que sejam parte da rotina das áreas de negócio da Enso; e

- Governança da Gestão de Risco: a eficácia da gestão de risco pela Enso quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

Ademais, no que se refere especificamente à segurança cibernética, a Enso identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- Malware – softwares desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, Spyware e Ransomware);

- Engenharia social – métodos de manipulação para obter informações confidenciais (Pharming, Phishing, Vishing, Smishing, e Acesso Pessoal);

- Ataques de DDoS (distributed denial of services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição;

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base no acima, a Enso avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

3.9. Ações de Prevenção e Proteção

Após a identificação dos riscos, a Enso adota as medidas a seguir descritas para proteger suas informações e sistemas.

- Regra Geral de Conduta:

A Enso realiza efetivo controle do acesso a arquivos que contemplem Informações Confidenciais em meio físico, disponibilizando-os somente aos Colaboradores que efetivamente estejam evolvidos no projeto que demanda o seu conhecimento e análise.

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Enso e circulem em ambientes externos à Enso com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas confidenciais.

A proibição acima referida não se aplica quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Enso. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

A troca de informações entre os Colaboradores da Enso deve sempre se pautar no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a Área de Compliance deve ser acionada previamente à revelação.

Neste sentido, os Colaboradores não deverão, em qualquer hipótese, deixar em suas respectivas estações de trabalho ou em outro espaço físico da Enso qualquer documento que contenha Informação Confidencial durante a ausência do respectivo usuário, principalmente após o encerramento do expediente.

Ademais, fica terminantemente proibido que os Colaboradores discutam ou acessem remotamente Informações Confidenciais.

Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Enso.

A Enso não mantém arquivo físico centralizado, sendo cada Colaborador responsável direto pela boa conservação, integridade e segurança de quaisquer informações em meio físico que tenha armazenadas consigo.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Os documentos físicos que contenham informações confidenciais ou de suas cópias deverão ser triturados e descartados imediatamente após seu uso de maneira a evitar sua recuperação ou leitura.
Em consonância com as normas internas acima, os Colaboradores devem se abster de utilizar pen-drivers, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva

para o desempenho de sua atividade na Enso. É proibida a conexão de equipamentos na rede da Enso que não estejam previamente autorizados pela área de informática e pelos administradores da Enso.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam difamar a imagem e afetar a reputação da Enso.

O recebimento de e-mails muitas vezes não depende do próprio Colaborador, mas espera-se bom senso de todos para, se possível, evitar receber mensagens com as características descritas previamente. Na eventualidade do recebimento de mensagens com as características acima descritas, o Colaborador deve apagá-las imediatamente, de modo que estas permaneçam o menor tempo possível nos computadores da Enso.

A visualização de sites, blogs, fotologs, webmails, entre outros, que contenham conteúdo discriminatório, preconceituoso (sobre origem, etnia, religião, classe social, opinião política, idade, sexo ou deficiência física), obsceno, pornográfico ou ofensivo é terminantemente proibida.

- Firewall, Software, Varreduras e Backup

A Enso utiliza um hardware de firewall projetado para evitar conexões não autorizadas e incursões maliciosas. O Diretor de Compliance, Risco e PLD é responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

A Enso mantém proteção atualizada contra malware nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem de forma maliciosa os sistemas da empresa (por exemplo, vírus, worms, spyware).

A Enso utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches.

A Enso mantém e testa regularmente medidas de backup consideradas apropriadas pelo Diretor de Compliance, Risco e PLD. As informações da Enso são atualmente objeto de backup diário com o uso de computação na nuvem.

3.10. Monitoramento e Testes

O Diretor de Compliance, Risco e PLD (ou pessoa por ele incumbida) adota as seguintes medidas para

monitorar determinados usos de dados e sistemas em um esforço para detectar acessos não autorizados ou outras violações potenciais, em base, no mínimo, trimestral:

(i) Monitoramento, por amostragem, do acesso dos Colaboradores a sites, blogs, fotologs, webmails, entre outros, bem como os e-mails enviados e recebidos;
(ii) Monitoramento, por amostragem, das ligações telefônicas dos seus Colaboradores realizadas ou recebidas por meio das linhas telefônicas disponibilizadas pela Enso para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Enso; e
(iii) Verificação, por amostragem, das informações de acesso a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento.

O Diretor de Compliance, Risco e PLD poderá adotar medidas adicionais para monitorar os sistemas de computação e os procedimentos aqui previstos para avaliar o seu cumprimento e sua eficácia.

3.11. Plano de Identificação e Resposta

- Identificação de Suspeitas

Qualquer suspeita de infecção, acesso não autorizado, outro comprometimento da rede ou dos dispositivos da Enso (incluindo qualquer violação efetiva ou potencial), ou ainda no caso de vazamento de quaisquer Informações Confidenciais, mesmo que de forma involuntária, deverá ser informada ao Diretor de Compliance, Risco e PLD prontamente. O Diretor de Compliance, Risco e PLD determinará quais membros da administração da Enso e, se aplicável, de agências reguladoras e de segurança pública, deverão ser notificados.

Ademais, o Diretor de Compliance, Risco e PLD determinará quais clientes ou investidores, se houver, deverão ser contatados com relação eventual à violação.

- Procedimentos de Resposta

O Diretor de Compliance, Risco e PLD responderá a qualquer informação de suspeita de infecção, acesso não autorizado ou outro comprometimento da rede ou dos dispositivos da Enso de acordo com os critérios abaixo:

(i) Avaliação do tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;

(ii) Identificação de quais sistemas, se houver, devem ser desconectados ou de outra forma

desabilitados;

(iii) Determinação dos papéis e responsabilidades do pessoal apropriado;

(iv) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;

(v) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);

(vi) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente, (por exemplo: em sendo Informações Confidenciais de fundo de investimento sob gestão da Enso, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);

(vii) Determinação do responsável (ou seja, a Enso ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do Diretor de Compliance, Risco e PLD, após a condução de investigação e uma avaliação completa das circunstâncias do incidente.

3.12. Arquivamento de Informações

De acordo com o disposto nesta Política, os Colaboradores deverão manter arquivada, pelo prazo regulamentar aplicável, toda e qualquer informação, bem como documentos e extratos que venham a ser necessários para a efetivação satisfatória de possível auditoria ou investigação em torno de possíveis investimentos e/ou clientes suspeitos de corrupção e/ou lavagem de dinheiro, em conformidade com o inciso II do § 8º do Artigo 4 da Resolução CVM nº 21.

3.13. Treinamento

O Diretor de Compliance, Risco e PLD organizará treinamento dos Colaboradores com relação às regras e procedimentos acima, conforme o disposto no Capítulo 4 desta Política de Controles Internos.

3.14. Revisão da Política

O Diretor de Compliance, Risco e PLD realizará uma revisão da Política de Segurança da Informação e Segurança Cibernética a cada 24 (vinte e quatro) meses, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Enso e acontecimentos regulatórios relevantes.

3.15. Penalidades

O descumprimento da presente Política implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

4. Programa de Treinamento

Competirá à Área de Compliance elaborar e implementar o calendário de treinamentos relacionado ao Código de Ética e Conduta da Enso e às demais políticas e manuais da Enso.

Os Colaboradores deverão participar de todos os treinamentos programados pela Área de Compliance, com o objetivo de atualizar seus conhecimentos acerca dos procedimentos e regras internas da Enso.

Cumpre ressaltar que a responsabilidade por treinar os Colaboradores de maneira a capacitá-los a exercer suas respectivas funções no âmbito das atividades desenvolvidas pelos setores da Enso recai sobre as lideranças de cada setor operacional da Enso, observada a Política de Certificação.

Desta forma, caberá à Área de Compliance assegurar a existência de treinamentos aos Colaboradores que garantam que os negócios da Enso sejam conduzidos de acordo com as regulações aplicáveis e melhores práticas de mercado. A implementação do processo de treinamento inicial e do programa de reciclagem continuada fica sob a responsabilidade do Diretor de Compliance, Risco e PLD e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

Tanto o processo de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Enso, seus princípios éticos e de conduta, as normas de Compliance, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Política (especialmente aquelas relativas à confidencialidade, segurança das informações, segurança cibernética e negociações pessoais), bem como as penalidades aplicáveis aos Colaboradores decorrentes do descumprimento de tais regras, além das principais leis e normas aplicáveis às referidas atividades.

O Diretor de Compliance, Risco e PLD poderá contratar profissionais especializados para conduzirem o treinamento inicial e programas de reciclagem, conforme as matérias a serem abordadas.

4.1 Treinamento e Processo de Reciclagem

A Enso possui um processo de treinamento **inicial** de todos os seus Colaboradores, especialmente aqueles que tenham acesso à Informações Confidenciais ou participem de processos de decisão de investimento, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

Assim que cada Colaborador for contratado, ele participará de um processo de treinamento em que irá adquirir conhecimento sobre as atividades da Enso e terá oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas.

Neste sentido, a Enso adota um programa de reciclagem **anual** dos seus Colaboradores, à medida que as normas, princípios, conceitos e valores contidos nesta Política sejam atualizados, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de reciclagem.

5. Política de Certificação

A Enso aderiu e está sujeita às disposições do Código ANBIMA de Regulação e Melhores Práticas para o Programa de Certificação Continuada ("Código ANBIMA de Certificação"), devendo garantir que todos os profissionais elegíveis estejam devidamente certificados.

5.1 Treinamento

A Enso incentiva o treinamento para seus Colaboradores, objetivando obter sua capacitação e desenvolvimento para aprimorar a qualidade do recurso humano no atendimento ao negócio.

Estimula-se o autotreinamento com supervisão, participação de reuniões internas, projetos e a liberdade de questionamentos e esclarecimento de dúvidas no ambiente interno.

5.2 Atividades Elegíveis e Critérios de Identificação para Certificação

Os Colaboradores que exercem atividades de administração de recursos de terceiros, conforme regulamentadas pelo Código ANBIMA de Certificação devem ter a Certificação de Gestores ANBIMA ("CGA") concedida por tal entidade.

Nesse sentido, a Enso definiu que apenas o Colaborador com poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão, conforme identificado no Formulário de Referência da Enso, ou seja, o Colaborador que tenha, de fato, alçada/poder discricionário de investimentos, é elegível à CGA.

A não aderência profissional aos requisitos mínimos com relação à certificação requerida implicará no afastamento do mesmo da atividade.

Caberá à área administrativa da Enso a identificação dos Colaboradores elegíveis a certificações, requerendo do Colaborador e ao seu superior imediato a certificação exigida na admissão ou na transferência de cargos que requerem certificações ou qualquer outro requisito mínimo estabelecido pelas entidades reguladoras do mercado. Deve, ainda manter relatório de controle sobre cargos, certificações e vencimentos das certificações, assim como a devida atualização e gestão dos cadastros e bancos de dados nas entidades reguladoras.

Todos os Colaboradores não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos nesta Política, serão, nos termos do art. 9º, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

5.3 Procedimentos

Os critérios que definem as atividades elegíveis às certificações são de acordo com a área de atuação na Enso e de acordo com o Código de Certificação da ANBIMA.

- **A identificação dos Colaboradores certificados na admissão e no desligamento**

A formalização das contratações e dos desligamentos de Colaboradores está sob responsabilidade da área administrativa. Para Colaboradores que mudam de área é requerida a certificação, desde que venha a deter o poder final para ordenar a compra ou venda de posições, sem a necessidade de aprovação prévia do Diretor de Gestão.
Antes da contratação, admissão ou transferência de área de qualquer Colaborador, a área administrativa da Enso deverá solicitar esclarecimentos ou confirmar junto ao supervisor direto do potencial Colaborador o cargo e as funções a serem desempenhadas, avaliando a necessidade de certificação, bem como verificar no Banco de Dados se o Colaborador possui alguma certificação ANBIMA, uma vez que, em caso positivo, a Enso deverá inserir o Colaborador no Banco de Dados da Enso.

O Diretor de Gestão deverá esclarecer à área administrativa da Enso se Colaboradores que integrarão o departamento técnico terão ou não alçada/poder discricionário de decisão de investimento.

Caso seja identificada a necessidade de certificação, a área administrativa da Enso deverá solicitar a comprovação da certificação pertinente ou sua isenção, se aplicável, anteriormente ao ingresso do novo Colaborador.

A área administrativa da Enso deverá checar se Colaboradores que estejam se desligando da Enso estão indicados no Banco de Dados da ANBIMA como profissionais elegíveis/certificados vinculados à Enso.

Todas as atualizações no Banco de Dados da ANBIMA devem ocorrer até o último dia útil do mês subsequente à data do evento que deu causa a atualização, nos termos do Art. 12, §1º, I do Código ANBIMA de Certificação, sendo que a manutenção das informações contidas no Banco de Dados deverá ser objeto de análise e confirmação pelo Diretor de Compliance, Risco e PLD, conforme disposto abaixo.

- **Vigências das Certificações**

Os mecanismos utilizados pela Enso para o controle de vencimento das certificações são:

A) Verificação periódica no site de certificação.
B) Controle em planilha Excel apenas com os Colaboradores certificados;

Os Colaboradores da área administrativa acompanham se o Colaborador certificado realizou ou não a atualização da certificação, e garante que este o faça dentro do prazo, através de novos avisos. Após a realização da atualização, o profissional envia o certificado à área administrativa.

5.4. Rotinas de Verificação

Mensalmente, o Diretor de Compliance, Risco e PLD deverá verificar as informações contidas no Banco de Dados da ANBIMA, a fim de garantir que todos os profissionais certificados/em processo de certificação, conforme aplicável, estejam devidamente identificados, bem como se as certificações estão dentro dos prazos de validade estabelecidos no Código ANBIMA de Certificação.
Ainda, o Diretor de Compliance, Risco e PLD deverá, mensalmente, contatar o Diretor de Gestão que deverá informá-lo se houve algum tipo de alteração nos cargos e funções dos Colaboradores que integram o departamento técnico envolvido na gestão de recursos, confirmando, ainda, todos aqueles Colaboradores que atuem com alçada/poder discricionário de investimento, se for o caso.

Colaboradores que não tenham CGA (e que não tenham a isenção concedida pelo Conselho de Certificação, nos termos do Art. 17 do Código ANBIMA de Certificação) estão impedidos de ordenar a compra e venda de ativos para os fundos de investimento sob gestão da Enso sem a aprovação prévia do Diretor de Gestão, tendo em vista que não possuem alçada/poder final de decisão para tanto.

Ademais, no curso das atividades de Compliance e fiscalização desempenhadas pelo Diretor de Compliance, Risco e PLD, caso seja verificada qualquer irregularidade com as funções exercidas por Colaborador, incluindo, sem limitação, a tomada de decisões de investimento sem autorização prévia do Diretor de Gestão por profissionais não certificados ou, de maneira geral, que o Colaborador está atuando em atividade elegível sem a certificação pertinente ou com a certificação vencida, o Diretor de Compliance, Risco e PLD deverá declarar, de imediato, o afastamento do Colaborador, devendo tal diretor, ainda, apurar potenciais irregularidades e eventual responsabilização dos envolvidos, inclusive dos superiores do Colaborador, conforme aplicável, bem como para traçar um plano de adequação.

Sem prejuízo do disposto acima, anualmente deverão ser discutidos os procedimentos e rotinas de verificação para cumprimento do Código de Certificação, sendo que as análises e eventuais recomendações, se for o caso, deverão ser objeto do relatório anual de Compliance.

Por fim, serão objeto do treinamento anual de Compliance assuntos de certificação, incluindo, sem limitação: (i) treinamento direcionado a todos os Colaboradores, descrevendo as certificações aplicáveis à atividade da Enso, suas principais características e os profissionais elegíveis; (ii) treinamento direcionado aos membros do departamento técnico envolvidos na atividade de gestão de recursos, reforçando que somente os Colaboradores com CGA podem ter alçada/poder discricionário de decisão de investimento em relação aos ativos integrantes das carteiras sob gestão da Enso, devendo os demais buscar aprovação junto ao Diretor de Gestão; (iii) treinamento direcionado aos Colaboradores da Área de Compliance, para que os mesmos tenham o conhecimento necessário para operar no Banco de Dados da ANBIMA e realizar as rotinas de verificação necessárias.

5.5. Processo de Afastamento

Todos os profissionais não certificados ou em processo de certificação, e para os quais a certificação seja exigível, nos termos previstos nesta Política, serão, nos termos do art. 9º, §1ª, inciso V do Código ANBIMA de Certificação, imediatamente afastados das atividades elegíveis aplicáveis, até que se certifiquem.

Os profissionais já certificados, caso deixem de ser Colaboradores da Enso, deverão assinar a documentação prevista no Anexo a esta Política denominado "Termo de Afastamento", comprovando o seu afastamento da Enso. O mesmo procedimento de assinatura do Anexo aqui em referência, será aplicável, de forma imediata, aos profissionais não certificados ou em processo de certificação que forem afastados por qualquer dos motivos acima mencionados.

6. Plano de Contingência e Continuidade de Negócios (PCN)

6.1. INTRODUÇÃO

O Plano de Continuidade de Negócios da Enso ("Plano de Contingência") tem como objetivo minimizar os danos e as perdas às atividades essenciais da empresa, desenvolvendo um conjunto de estratégias de forma a garantir que os serviços possam ser executados de forma contínua e ininterrupta durante o processo de contingência.

A Enso possui um plano que visa permitir que após um processo de ativação de contingência possa-se reassumir o processamento das operações críticas enquanto o processo de contingência se mantiver.

Ainda, o plano prevê também as medidas tomadas em caso de saída de algum dos diretores estatutários da Enso, cuja indicação seja obrigatória para fins de atendimento às normas às quais a Enso está sujeita. Em caso de ocorrência da situação, uma reunião extraordinária de sócios deverá ser realizada a fim de se definir o novo diretor.

Adicionalmente, o Plano de Contingência tem como objetivo definir os procedimentos a serem adotados pela equipe da Enso, no caso de contingência, de modo a impedir descontinuidade operacional por problemas que impactem no funcionamento da Enso no âmbito da sua atividade de gestão de recursos. Foram estipulados estratégias e planos de ação com o intuito de garantir que os serviços essenciais da Enso sejam devidamente identificados e preservados após a ocorrência de um imprevisto ou um desastre.

Essas situações são classificadas de forma geral como contingências e implicam na modificação da rotina diária da operação, o que pode causar impactos financeiros, legais/regulatórios e de imagem, entre outros, à Enso.

6.2. ESTRUTURA

Para atendimento às necessidades mínimas de manutenção dos serviços/atividades da Enso, foi definida uma estrutura mínima física, tecnológica e de pessoal, e procedimentos que devem ser adotados toda vez em que uma situação seja caracterizada como uma contingência às operações da Enso.

Foram identificados os seguintes focos de preocupação relativos à atividade de gestão de recursos que necessitam estar contemplados neste Plano de Contingência, de forma a garantir o regular funcionamento da Enso:

(i) Espaço Físico: local onde são realizadas as operações da Enso. Nesse espaço encontra-se instalada toda a infraestrutura necessária para a execução de suas atividades de gestão de recursos;

(ii) Tecnologia: fundamental para o funcionamento da Enso relativamente à gestão de recursos, no sentido de que todas as comunicações com clientes, corretoras, administradores de fundos etc., são realizados por telefone ou meios eletrônicos (e-mails e/ou sistemas próprios). Também é fundamental para a realização de registros de operações (compras e vendas de títulos, aplicações e resgates em fundos de investimento, transferência de recursos e pagamento de despesas da Enso, dentro outros); e

(iii) Pessoal: responsáveis pela operação da Enso, incluindo a análise e decisão para realização ou não de investimentos, equipe responsável pelo Compliance e pela gestão de risco das carteiras etc.

Tendo identificado esses 3 (três) focos de preocupação do ponto de vista da estrutura da Enso e dos processos sob sua responsabilidade na qualidade de gestora de recursos, os riscos que podem ocasionar o acionamento do Plano de Contingência foram identificados da seguinte forma:

(i) Problemas de Infraestrutura: os problemas dessa ordem são, dentre outros, falta de energia elétrica, falha nos links de internet, falha nas linhas telefônicas, falhas nos sites das empresas que fornecem sistemas de uso da Enso, falta de água etc.;

(ii) Problemas de acesso ao local/recursos: os problemas dessa ordem são, dentre outros, impossibilidade ou dificuldade de acesso ao local onde se localiza o escritório. Essa impossibilidade pode ser causada por eventos como greves, greves de transporte público, interdições pelas autoridades do prédio ou do entorno do escritório da Enso etc.; e

(iii) Falta impactante de colaboradores: os problemas dessa ordem são, dentre outros, o término de vínculo repentino com pessoas chave para o funcionamento da Enso

(notadamente seus diretores), o não comparecimento de número expressivo de colaboradores em razão de doenças ou qualquer outro tipo de impedimento etc.

Com base no levantamento da estrutura da Enso relativa à gestão de recursos e no mapeamento de riscos, a Enso tem condições de manter sua atuação mesmo na impossibilidade de acesso às suas instalações e/ou no caso de falta impactante de colaboradores ao local de trabalho.

Conforme avaliação de risco da Enso foram definidas as seguintes ações a serem tomadas quando da ativação do Plano de Contingência da Enso:

(i) Ambiente Físico

O ambiente físico é definido como o espaço onde as operações diárias de gestão de recursos da Enso são conduzidas normalmente. Esse espaço inclui o imóvel, os móveis e utensílios necessários a essa operação, como também o acesso seguro a esses recursos.

Em ocorrendo situações de problemas de acesso às suas dependências, a equipe da Enso deve continuar a desempenhar suas atividades através de Home Office. Além disso, há a vinculação dos e-mails e armazenamento em plataforma em nuvem. Assim, é possível permanecer trabalhando ainda que fora do escritório da ENSO.

(ii) Ambiente Tecnológico

O ambiente tecnológico envolve todos os sistemas e recursos necessários para que a Enso possa realizar sua operação de forma normal. Isso implica basicamente a disponibilidade de acesso aos sistemas utilizados pela Enso para a gestão de recursos em seu dia a dia e garantira de que suas informações estejam protegidas e possam ser acessadas e/ou utilizadas na operação da Enso, que inclui o armazenamento de dados de sistemas e aplicativos, os equipamentos eletrônicos em geral, links de telecomunicação e transmissão de dados, softwares e computadores, aparelhos telefônicos etc., incluindo os recursos necessários para que tais itens funcionem de forma adequada e segura.

A Enso conta com práticas de alta disponibilidade em sua infraestrutura de tecnologia de informação. Toda a infraestrutura física de tecnologia da Enso é coberta por nobreaks para garantir a continuidade das operações em caso de queda da energia elétrica. Contando também com redundância de links de internet para incrementar a disponibilidade nesta.

Todos os sistemas utilizados pela ENSO são acessados através de sites dos próprios provedores desses sistemas, o que viabiliza acessá-los de qualquer local desde que se disponha de um computador com um link de internet.

Diariamente são realizados backups dos dados armazenados na "nuvem" em servidores internos, possibilitando acesso aos dados em caso de indisponibilidade de comunicação com o sistema.

A comunicação com clientes, corretoras, parceiros e administradores poderá continuar sendo realizada através da utilização de telefones celulares da equipe da Enso. Para tanto, há procedimento de comunicar a esses terceiros o estado de contingência da Enso, de forma a que estes também tenham conhecimento da situação tão logo ela ocorra, buscando impactar o mínimo possível a operação de gestão de recursos da Enso.

(iii) Ambiente Pessoal

O ambiente pessoal envolve todos os colaboradores e prestadores de serviços existentes na Enso relacionados à atividade de gestão de recursos. Suas funções devem atender às necessidades de funcionamento da Enso em situações consideradas de normalidade bem como em situações consideradas de contingência.

Este Plano de Contingência visa atribuir prioridades e responsabilidades à equipe da Enso de forma a impactar o mínimo possível em suas atividades em situação de contingência.

O principal ponto identificado de risco é a não existência de um backup de atividades executadas por um determinado funcionário. Esse risco, no entanto, não é considerado como relevante pois a estrutura da Enso já conta hoje com a definição e treinamento dos funcionários para atuação como backup das funções e responsabilidades de seus colegas de Enso. Tal medida já existe e é praticada regularmente quando, por exemplo, um determinado colaborador se ausenta da Enso (por férias ou licença) e suas atividades continuam sendo executadas pelo seu backup designado.

6.3. EQUIPE DE CONTINGÊNCIA

Para coordenar todas as ações necessárias em situações de contingência bem como promover o adequado treinamento e ações para restabelecimento da situação de atividade normal da Enso, foram definidos os seguintes responsáveis pela Equipe de Contingência:

- Diretor de Compliance, Risco e PLD (Coordenador de Contingência); e
- Diretor de Gestão, conforme definido no Formulário de Referência da Enso.

Essas pessoas deverão tomar as decisões necessárias para acionar este Plano de Contingência se e quando necessário, tomando essa decisão em conjunto ou, no caso de impossibilidade, com os demais administradores da Enso.

6.4. CENÁRIOS DE CONTINGÊNCIA

Neste cenário, considera-se basicamente a impossibilidade ou dificuldade em manter o funcionamento normal da Enso devido a problemas de ordem técnica (hardware/software), física (acesso ao escritório), pessoal (ausência significativa de colaboradores) e de infraestrutura (falta de energia).

Nessa situação, o Coordenador de Contingência deverá acionar este Plano de Contingência, em caráter imediato, e iniciar também imediatamente a avaliação das causas que geraram a contingência para providenciar sua solução o mais rapidamente possível, bem como dar início ao efetivo cumprimento dos procedimentos descritos abaixo, quais sejam:

(a) Comunicar imediatamente o ocorrido à toda a equipe interna, via ligação celular, grupo corporativo da empresa em aplicativo de mensagens ou qualquer outro meio à sua disposição, indicando nessa oportunidade qual o procedimento a ser adotado por cada colaborador de acordo com a contingência ocorrida;

(b) Caso seja verificada a necessidade de sair do escritório da Enso, os colaboradores poderão continuar a desempenhar suas atividades através de Home Office. A continuidade das operações da ENSO deverá ser assegurada no próprio dia útil da ocorrência da contingência no escritório físico, de modo que as atividades diárias não sejam interrompidas ou gravemente impactadas.

O Coordenador de Contingência deverá acompanhar todo o processo acima descrito até o retorno à situação normal de funcionamento dentro do contexto das atividades desempenhadas pela ENSO e reportar eventuais alterações e atualizações da contingência aos demais colaboradores.

6.5. ASPECTOS GERAIS

Este Plano de Contingência é de uso restrito dos colaboradores da Enso e **não** pode ser divulgado para terceiros, exceto se autorizado pela Equipe de Contingência.

É responsabilidade do Coordenador de Contingência manter este Plano atualizado, bem como a realização de validação **anual** dos procedimentos estabelecidos neste Plano de Contingência.

Ainda, o Coordenador de Contingência realizará testes de contingências que possibilitem que a Enso esteja preparada para eventos desta natureza, proporcionando à Enso condições adequadas para continuar suas operações.

Sendo assim, **anualmente**, é realizado um teste de contingência para verificar:

a) Acesso aos sistemas;
b) Acesso ao e-mail corporativo;
c) Acesso aos dados armazenados;
d) Verificação do treinamento aos colaboradores para atuarem como back-up; e
e) Qualquer outra atividade necessária para continuidade do negócio.

O resultado do teste é registrado em relatório, que servirá como indicador para regularização das possíveis falhas identificadas, servindo como apoio ao constante aprimoramento deste Plano de Contingência.

7. Política de Sustentabilidade

A Enso deve sempre buscar adotar práticas e ações sustentáveis para minimizar eventuais impactos ambientais, incluindo, mas não se limitando a: (a) utilização de papel reciclável para impressão de documentos; (b) utilização de refil de cartuchos e toners para impressão; (c) separação do material reciclável para fins de coleta seletiva de lixo; (d) utilização de lâmpadas de baixo consumo energético; e (e) incentivo à utilização de meios de transporte alternativos ou de menor impacto ambiental por seus Colaboradores, como transportes coletivos, caronas ou bicicletas.

Além disso, a Enso incentiva seus Colaboradores a adotar postura semelhante no dia a dia de suas atividades, por exemplo: (a) evitar imprimir e-mails e arquivos eletrônicos, exceto se necessário; (b) optar por utilizar canecas ou copos reutilizáveis; (c) desligar os computadores todos os dias ao final do expediente; (d) apagar as luzes das salas ao sair; e (e) desligar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso.

8. Política Anticorrupção

8.1. Introdução

A Enso está sujeita às leis e normas de anticorrupção, incluindo, mas não se limitando, à Lei nº 12.846/13 e Decreto nº 8.420/15 ("Normas de Anticorrupção").

Qualquer violação desta Política de Anticorrupção e das Normas de Anticorrupção pode resultar em penalidades civis e administrativas severas para a Enso e/ou seus Colaboradores, bem como impactos de ordem reputacional, sem prejuízo de eventual responsabilidade criminal dos indivíduos envolvidos.

8.2. Abrangência das Normas de Anticorrupção

As Normas de Anticorrupção estabelecem que as pessoas jurídicas serão responsabilizadas objetivamente, nos âmbitos administrativo e civil, pelos atos lesivos praticados por seus sócios e colaboradores contra a administração pública, nacional ou estrangeira, sem prejuízo da responsabilidade individual do autor, coautor ou partícipe do ato ilícito, na medida de sua culpabilidade.

Considera-se agente público e, portanto, sujeito às Normas de Anticorrupção, sem limitação: (i) qualquer indivíduo que, mesmo que temporariamente e sem compensação, esteja a serviço, empregado ou mantendo uma função pública em entidade governamental, entidade controlada pelo governo, ou entidade de propriedade do governo; (ii) qualquer indivíduo que seja candidato ou esteja ocupando um cargo público; e (iii) qualquer partido político ou representante de partido político.

Considera-se administração pública estrangeira os órgãos e entidades estatais ou representações diplomáticas de país estrangeiro, de qualquer nível ou esfera de governo, bem como as pessoas jurídicas controladas, direta ou indiretamente, pelo poder público de país estrangeiro e as organizações públicas internacionais.

As mesmas exigências e restrições também se aplicam aos familiares de funcionários públicos até o segundo grau (cônjuges, filhos e enteados, pais, avós, irmãos, tios e sobrinhos).

Representantes de fundos de pensão públicos, cartorários e assessores de funcionários públicos também devem ser considerados “agentes públicos” para os propósitos desta Política de Anticorrupção e das Normas de Anticorrupção.

8.3. Definição

Nos termos das Normas de Anticorrupção, constituem atos lesivos contra a administração pública, nacional ou estrangeira, todos aqueles que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil, assim definidos:

I prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos nas Normas de Anticorrupção;

III comprovadamente utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV no tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) fraudar licitação pública ou contrato dela decorrente;

e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública.

V dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

8.4. <u>Normas de Conduta</u>

É terminantemente proibido dar ou oferecer qualquer valor ou presente a agente público sem autorização prévia do Diretor de Compliance, Risco e PLD.

Os Colaboradores deverão se atentar, ainda, que (i) qualquer valor oferecido a agentes públicos, por menor que seja, poderá caracterizar violação às Normas de Anticorrupção e ensejar a aplicação das penalidades previstas; e (ii) a violação às Normas de Anticorrupção estará configurada mesmo que a oferta de suborno seja recusada pelo agente público.

Os Colaboradores deverão questionar a legitimidade de quaisquer pagamentos solicitados pelas autoridades ou funcionários públicos que não encontram previsão legal ou regulamentar.

Nenhum sócio ou colaborador poderá ser penalizado devido a atraso ou perda de negócios resultantes de sua recusa em pagar ou oferecer suborno a agentes públicos.

8.5. Proibição de Doações Eleitorais

A Enso não fará, em hipótese alguma, doação a candidatos e/ou partidos políticos via pessoa jurídica. Em relação às doações individuais dos Colaboradores, a Enso e seus Colaboradores têm a obrigação de seguir estritamente a legislação vigente.

8.6. Relacionamentos com Agentes Públicos

Quando se fizer necessária a realização de reuniões e audiências ("Audiências") com agentes públicos, sejam elas internas ou externas, a Enso será representada por, ao menos, 2 (dois) Colaboradores, que deverão se certificar de empregar a cautela exigida para a ocasião, com o objetivo de resguardar a Enso contra condutas ilícitas no relacionamento com agentes públicos. Dentre os procedimentos adotados, os Colaboradores que estiverem representando a Enso deverão elaborar relatórios de tais Audiências, e os apresentar ao Diretor de Compliance, Risco e PLD imediatamente após sua ocorrência.

9. Controle de Versões

Esta Política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.

Versão	Data	Modificado por:	Descrição
1.0	23/05/2019	Diretor de Compliance	Criação do documento
2.0	07/08/2019	Diretor de Compliance	Aprimoramento
3.0	29/11/2019	Diretor de Compliance	Aprimoramento
4.0	05/06/2020	Diretor de Compliance, Risco e PLD	Adequação ao Código ANBIMA de Administração de Recursos de Terceiros
5.0	09/12/2021	Diretor de Compliance, Risco e PLD	Mudança identidade visual; Atualização do item 3.9
6.0	12/04/2023	Diretor de Compliance, Risco e PLD	Revisão geral e migração dos capítulos de conflito de interesses, segregação e soft dólar para o Código de Ética.

ANEXO I
TERMO DE RECEBIMENTO E COMPROMISSO

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, DECLARO para os devidos fins:

(i) Ter recebido, na presente data, a Política de Regras Procedimentos e Controles Internos atualizado ("Política") da **ENSO GESTÃO DE RECURSOS LTDA.** ("Enso");
(ii) Ter lido, sanado todas as minhas dúvidas e entendido integralmente as disposições constantes na Política;
(iii) Estar ciente de que a Política como um todo passa a fazer parte dos meus deveres como Colaborador da Enso, incorporando-se às demais regras internas adotadas pela Enso; e
(iv) Estar ciente do seu compromisso de comunicar ao Diretor de Compliance, Risco e PLD da Enso qualquer situação que chegue ao meu conhecimento que esteja em desacordo com as regras definidas nesta Política.

[local], [data].

_____
[**COLABORADOR**]

ANEXO II
TERMO DE CONFIDENCIALIDADE

Por meio deste instrumento eu, _____, inscrito no CPF/ME sob o nº _____, doravante denominado Colaborador, e **ENSO GESTÃO DE RECURSOS LTDA.** ("Enso").

Resolvem as partes, para fim de preservação de informações pessoais e profissionais dos clientes e da Enso, celebrar o presente termo de confidencialidade ("Termo"), que deve ser regido de acordo com as cláusulas que seguem:

1. São consideradas informações confidenciais, reservadas ou privilegiadas ("Informações Confidenciais"), para os fins deste Termo, independente destas informações estarem contidas em discos, disquetes, pen-drives, fitas, outros tipos de mídia ou em documentos físicos, ou serem escritas, verbais ou apresentadas de modo tangível ou intangível, qualquer informação sobre a Enso, seus sócios e clientes, aqui também contemplados os próprios FUNDOS, incluindo:

a) Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
b) Informações técnicas, financeiras ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes, dos clubes, fundos de investimento e carteiras geridas pela Enso, conforme aplicável;
c) Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os clubes, fundos de investimento e carteiras geridas pela ENSO, conforme aplicável;
d) Informações estratégicas ou mercadológicas e outras, de qualquer natureza, obtidas junto a sócios, sócios-diretores, funcionários, trainees ou estagiários da Enso ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Enso e que ainda não foi devidamente levado à público;
e) Informações a respeito de resultados financeiros antes da publicação dos balanços e balancetes dos fundos;
f) Transações realizadas e que ainda não tenham sido divulgadas publicamente; e
g) Outras informações obtidas junto a sócios, diretores, funcionários, trainees ou estagiários da Enso ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

2. O Colaborador compromete-se a utilizar as Informações Confidenciais a que venha a ter acesso estrita e exclusivamente para desempenho de suas atividades na Enso, comprometendo-se, portanto, a não divulgar tais Informações Confidenciais para quaisquer fins, Colaboradores não autorizados, mídia, ou pessoas estranhas à Enso, inclusive, nesse último caso, cônjuge, companheiro(a), ascendente, descendente, qualquer pessoa de relacionamento próximo ou dependente financeiro do Colaborador.

2.1. O Colaborador se obriga a, durante a vigência deste Termo e por prazo indeterminado após sua rescisão, manter absoluto sigilo pessoal e profissional das Informações Confidenciais a que teve acesso durante o seu período na Enso, se comprometendo, ainda a não utilizar, praticar ou divulgar Informações Confidenciais, "Insider Trading", "Dicas" e "Front Running", seja atuando em benefício próprio, da Enso ou de terceiros.

2.2. A não observância da confidencialidade e do sigilo, mesmo após o término da vigência deste Termo, estará sujeita à responsabilização nas esferas cível e criminal.

3. O Colaborador entende que a revelação não autorizada de qualquer Informação Confidencial pode acarretar prejuízos irreparáveis, ficando deste já o Colaborador obrigado a indenizar a Enso, seus sócios e terceiros prejudicados, nos termos estabelecidos a seguir.

3.1. O descumprimento acima estabelecido será considerado ilícito civil e criminal, ensejando inclusive sua classificação como justa causa para efeitos de rescisão de contrato de trabalho, quando aplicável, nos termos do artigo 482 da Consolidação das Leis de Trabalho.

3.2. O Colaborador tem ciência de que terá a responsabilidade de provar que a informação divulgada indevidamente não se trata de Informação Confidencial.

4. O Colaborador reconhece e toma ciência que:

(i) Todos os documentos relacionados direta ou indiretamente com as Informações Confidenciais, inclusive contratos, minutas de contrato, cartas, fac-símiles, apresentações a clientes, e-mails e todo tipo de correspondências eletrônicas, arquivos e sistemas computadorizados, planilhas, planos de ação, modelos de avaliação, análise, gestão e memorandos por este elaborados ou obtidos em decorrência do desempenho de suas atividades na Enso são e permanecerão sendo propriedade exclusiva da Enso e de seus sócios, razão pela qual compromete-se a não utilizar tais documentos, no presente ou no futuro, para quaisquer fins que não o desempenho de suas atividades na Enso, devendo todos os documentos permanecer em poder e sob a custódia da Enso, salvo se em virtude de interesses da Enso for

necessário que o Colaborador mantenha guarda de tais documentos ou de suas cópias fora das instalações da Enso;

(ii) Em caso de rescisão do contrato individual de trabalho, desligamento ou exclusão do Colaborador, o Colaborador deverá restituir imediatamente à Enso todos os documentos e cópias que contenham Informações Confidenciais que estejam em seu poder;

(iii) Nos termos da Lei 9.609/98, a base de dados, sistemas computadorizados desenvolvidos internamente, modelos computadorizados de análise, avaliação e gestão de qualquer natureza, bem como arquivos eletrônicos, são de propriedade exclusiva da Enso, sendo terminantemente proibida sua reprodução total ou parcial, por qualquer meio ou processo; sua tradução, adaptação, reordenação ou qualquer outra modificação; a distribuição do original ou cópias da base de dados ou a sua comunicação ao público; a reprodução, a distribuição ou comunicação ao público de informações parciais, dos resultados das operações relacionadas à base de dados ou, ainda, a disseminação de boatos, ficando sujeito, em caso de infração, às penalidades dispostas na referida lei.

5. Ocorrendo a hipótese do Colaborador ser requisitado por autoridades brasileiras ou estrangeiras (em perguntas orais, interrogatórios, pedidos de informação ou documentos, notificações, citações ou intimações, e investigações de qualquer natureza) a divulgar qualquer Informação Confidencial a que teve acesso, o Colaborador deverá notificar imediatamente a Enso, permitindo que a Enso procure a medida judicial cabível para atender ou evitar a revelação.

5.1. Caso a Enso não consiga a ordem judicial para impedir a revelação das informações em tempo hábil, o Colaborador poderá fornecer a Informação Confidencial solicitada pela autoridade. Nesse caso, o fornecimento da Informação Confidencial solicitada deverá restringir-se exclusivamente àquela que o Colaborador esteja obrigado a divulgar.

5.2. A obrigação de notificar a Enso subsiste mesmo depois de rescindido o contrato individual de trabalho, ao desligamento ou exclusão do Colaborador, por prazo indeterminado.

6. Este Termo é parte integrante das regras que regem a relação contratual e/ou societária do Colaborador com a Enso, que ao assiná-lo está aceitando expressamente os termos e condições aqui estabelecidos.

7. A transgressão a qualquer das regras descritas neste Termo, sem prejuízo do disposto no item 3 e seguintes acima, será considerada infração contratual, sujeitando o Colaborador às sanções que lhe forem atribuídas pelos sócios da Enso.

Assim, estando de acordo com as condições acima mencionadas, assinam o presente em 02 (duas) vias de igual teor e forma, para um só efeito produzirem, na presença das testemunhas abaixo assinadas.

[local], [data].

_____

[COLABORADOR]

_____

ENSO GESTÃO DE RECURSOS LTDA.

Testemunhas:

1._____ 2._____

Nome: Nome:

CPF: CPF:

ANEXO III
TERMO DE AFASTAMENTO

Por meio deste instrumento, eu, _____, inscrito(a) no CPF/ME sob o nº _____, declaro para os devidos fins que, a partir desta data, estou afastado das atividades de gestão de recursos de terceiros da **ENSO GESTÃO DE RECURSOS LTDA**. ("ENSO") por prazo indeterminado:

[ ] até que me certifique pela CGA, no caso da atividade de gestão de recursos de terceiros com alçada/poder discricionário de investimento;

[ ] ou até que o Conselho de Certificação, nos termos do Art. 17 do Código de Certificação, me conceda a isenção de obtenção da CGA;

[ ] tendo em vista que não sou mais Colaborador da Enso;

São Paulo, [---] de [---] de [---].

_____
[COLABORADOR]

_____
ENSO GESTÃO DE RECURSOS LTDA.

Testemunhas:

1._____ 2._____
Nome: Nome:
CPF: CPF: