

## **CÓDIGO DE ÉTICA SYSTEM MANAGER:**

### **Mensagem do Presidente**

Neste mundo onde colecionamos desafios, vitórias e as vezes até mesmo derrotas, cada um de nós tomamos decisões de negócios algumas muito simples e outras muito mais complexas, independentemente da situação temos a missão de contemplar através de uma jornada diária construirmos juntos uma empresa responsável e ética que preza pela excelência do trabalho, colocando nossos clientes, colaboradores e fornecedores no centro e sempre seguindo nossos princípios éticos descritos neste Código de ética e Conduta.

O mundo hoje preza pela transparência, credibilidade e pelas boas práticas e na SYSTEM MANAGER não poderia ser diferente. A empresa é feita por pessoas e são suas condutas que traçam a credibilidade de uma organização.

Por isso, decidimos nos tornar uma fonte inesgotável de ética e confiabilidade de produtos e serviços de tecnologia.

Os valores da System Manager são a base sobre a qual esta empresa foi construída e continua a prosperar. É importante que cada um de nós entendamos e vivamos os valores da System Manager, eles orientam nossas interações com os clientes, fornecedores, colegas de trabalho, comunidades nas quais operamos.

Somos uma empresa com operações em diferentes ambientes culturais, políticos e econômicos. Em todas as nossas operações, os valores da System Manager e a nossa integridade continuam sendo nosso objetivo.

Sempre lutamos para melhorar nosso desempenho e agregar valor aos envolvidos na Companhia; são esses objetivos que são decisivos para o nosso constante sucesso. Embora atingir metas financeiras e operacionais sejam muito importantes, devemos sempre lutar para alcançar tais objetivos de acordo com as leis e regulamentos aplicáveis e de acordo com os nossos valores.

**Leandro Silva**  
**CEO**

## Sumário

1. OBJETIVO DO CÓDIGO:	4
2. INTRODUÇÃO AO CÓDIGO DE ÉTICA	4
3. ABRANGÊNCIA	5
4. PRINCÍPIOS GERAIS	6
5. Controles Internos:	7
6. Política da Empresa:	9
7. Gerenciamento de Risco Operacional	9
8. Controles Administrativos:	10
9. Controles Contábeis:	10
10. Controles de gestão do Recursos Humanos:	10
11. Compliance:	11
12. Código de Ética e Conduta Bem Definido:	11
a) Prevenir:	12
b) Detectar	12
c) Corrigir	12
13. PROGRAMA DE GOVERNANÇA CORPORATIVA:	13
14. LIDERANÇA ÉTICA E INTEGRIDADE:	15
15. Diretrizes de Conformidade:	16
16. Due Diligence	17
17. NORMAS DE CONDUTA	19
18. CONDUITAS REPROVÁVEIS	19
19. CONDUITAS ESPERADAS	20
20. RELACIONAMENTO COM AS PARTES INTERESSADAS	20
22. COLABORADORES	21
23. FORNECEDORES	21
24. CONCORRENTES	22
25. DO JURÍDICO:	22
26. COM OS ÓRGÃOS REGULADORES, FISCALIZADORES E GOVERNO:	22
27. PÚBLICO, SOCIEDADE E COMUNIDADE	23
28. PARCEIROS	23
30. LEI GERAL DE PROTEÇÃO DE DADOS:	25
31. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	26
32. Propriedade intelectual:	28

33.	Direitos autorais: .....	28
34.	POLÍTICA DE SUSTENTABILIDADE:.....	29
35.	GESTÃO DO CÓDIGO DE ÉTICA .....	29
36.	Missão, Visão e Valores da System Manager: .....	29
37.	POLÍTICA ANTI - CORRUPÇÃO E SUBORNO .....	30
38.	Conceitos e Aplicação das Leis Anticorrupção(12.846/13). .....	33
39.	POLÍTICA DE PREVENÇÃO A FRAUDES: .....	34
a)	Objetivo .....	34
b)	Âmbito .....	34
c)	Definições.....	34
d)	Responsabilidades .....	35
e)	Medidas Preventivas .....	35
f)	Processo de Denúncia .....	35
40.	PRESENTES E ENTRETENIMENTO .....	35
41.	PROFISSIONALISMO E ASSÉDIO.....	36
42.	Respeito e tratamento justo.....	37
43.	Participação em associações de classe e eventos do setor:.....	37
44.	Política de Qualidade: .....	37
45.	PROTEÇÃO DA MARCA: .....	38
46.	SAÚDE, SEGURANÇA E MEIO-AMBIENTE .....	38
47.	PROIBIÇÃO DE DOAÇÕES ELEITORAIS:.....	38
48.	Canal Direto de Conduta e Denúncias .....	39

## PROGRAMA DE ÉTICA E DE CONDUTA DA SYSTEM MANAGER

Mencionar as diretrizes de cada cargo e função, CEO, DIRETORIA, CONSELHO, etc.

### 1. OBJETIVO DO CÓDIGO:

O objetivo primordial deste Código é conscientizar os colaboradores da importância que a conduta ética tem para a empresa e como ela pode ser atingida. A companhia sabe que só com base no comportamento ético de seus colaboradores é que pode afirmar ser uma empresa compromissada com tais valores.

O desenvolvimento e evolução dos negócios da companhia dependem dos colaboradores, que estes conduzam suas atividades com o mais elevado grau de comprometimento, em plena conformidade com a legislação, normas e regulamentos aplicáveis, portando-se sempre com ética e moral, cumprindo a lei e o disposto neste Código e nas demais políticas internas.

A finalidade deste Código de Ética é servir como Guia Prático de Conduta Pessoal e Profissional, a ser utilizado por todos os funcionários da System Manager em suas relações e decisões diárias, tornando claros os nossos princípios e afirmando nossos valores.

Aplica-se a todos os administradores e Colaboradores da Empresa.

### 2. INTRODUÇÃO AO CÓDIGO DE ÉTICA

Nossa conduta depende do desempenho de todas as pessoas da Empresa, que devem seguir os padrões éticos pelos quais são incentivados e responsabilizados, regidos pelos seguintes princípios:

- Disseminar a cultura ética e de controles;
- Reforçar a importância da honestidade, humildade e companheirismo em nossas relações;
- Indicar condutas e comportamentos esperados; e
- Orientar todos como identificar e tratar condutas indesejadas, ilegais ou antiéticas.
- Respeitar a dignidade das pessoas, integridade e privacidade dos nossos clientes, acionistas, colegas, prestadores de serviços contratados em regime de terceirização, fornecedores, concorrentes e entidades de direito público;
- Cumprir as leis, normas e regulamentos aplicáveis;
- Preservar o patrimônio e a imagem da empresa;
- Agir com responsabilidade, de modo a conquistar e manter a confiança de todos;
- Cooperar para que sejam atingidos os objetivos da Empresa;

- Usar as informações recebidas exclusivamente no exercício do seu trabalho;
- Recusar vantagens que tenham por objetivo influenciar decisões na atuação profissional;
- Evitar qualquer forma de constrangimento às pessoas no ambiente de trabalho;
- Manter sigilo sobre as operações e estratégias da System Manager.

Considerando que dificilmente um código de ética abrange todas as situações encontradas na prática, acreditamos no seu senso de julgamento e o incentivamos a consultar, em caso de dúvidas, outros colaboradores ou diretamente algum membro da Diretoria.

### **3. ABRANGÊNCIA**

Este Código de Ética aplica-se aos funcionários da System Manager, seus contratados e terceirizados, que chamaremos de colaboradores neste documento.

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

Este Manual também é parte integrante das regras que regem a relação societária ou de trabalho dos Colaboradores, os quais, ao assinar o termo contratual e de 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 empresa neste manual.

Para melhor referência dos Colaboradores, as principais normas aplicáveis às atividades da Companhia.

Todo Colaborador, firmará o Termo de Compromisso e Ética dentro da empresa

Por meio desse documento, o Colaborador reconhece e confirma seu conhecimento e concordância com os termos deste Manual 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 Compromisso, reforçando o conhecimento e concordância com os termos deste Manual.

O descumprimento, suspeita ou indício de descumprimento de quaisquer das normas, princípios, conceitos e valores estabelecidos neste Manual ou das demais normas aplicáveis às atividades da Companhia, deverá ser levado para apreciação da área de Compliance e ao setor de Recursos Humanos, abaixo definido, de acordo com os procedimentos estabelecidos neste Manual.

Competirá a área de Compliance, e ao setor de Recursos Humanos aplicar as sanções decorrentes de tais desvios, nos termos deste Manual, garantido ao Colaborador amplo direito de defesa.

É dever de todo Colaborador informar a área de Compliance, sobre violações ou possíveis violações dos princípios e normas aqui dispostos, de maneira a preservar os interesses dos clientes da Companhia, bem como zelar pela reputação da empresa.

Caso a violação ou suspeita de violação recaia sobre o própria área de Compliance o Colaborador deverá informar diretamente aos demais administradores da Empresa.

#### **4. PRINCÍPIOS GERAIS**

Embora apresente diversas regras, diretrizes e exemplos de práticas e condutas que fazem parte de nosso dia a dia, este Código nunca conseguirá substituir o bom senso e comportamento responsável de um profissional, tampouco prever ou trazer respostas prontas para todas as situações ocorridas internamente, na execução de negócios ou perante a sociedade.

A System Manager sempre pautou sua atuação por princípios éticos compartilhados por todos os colaboradores da organização.

A System Manager tem por princípio a defesa e o fortalecimento das atividades

empresariais, dentro dos princípios da livre iniciativa. Destaca-se entre os seus objetivos, o de manter a reputação de entidade sólida e confiável, consciente de sua responsabilidade social e empresarial, agindo sempre de forma idônea, justa, legal e transparente.

Sua ação é marcada pela integridade, confiança e lealdade, bem como pelo respeito e valorização do ser humano, em sua privacidade, individualidade e dignidade. Repudia qualquer atitude guiada por preconceitos relacionados com origem, raça, religião, classe social, sexo, opção sexual, cor, idade, incapacidade física e quaisquer outras formas de discriminação.

A System Manager não aceita, tanto dentro da empresa quanto com fornecedores e parceiros de negócios, trabalho escravo ou em condição análoga, bem como uso de mão de obra infantil.

A System manager não trabalhará com qualquer parceiro comercial que opere mediante tratamento inaceitável de empregado, como punição física, abuso feminino, servidão involuntária e outras formas de abuso.

Os colaboradores devem ter o compromisso de zelar pelos valores e pela imagem da System Manager e manter a postura compatível com essa imagem.

Os princípios éticos de atuação da System Manager visam nortear o comportamento e a conduta de todos os colaboradores e, como nem tudo estará escrito, em caso de dúvidas, direcione-as ao seu gestor ou à área de Compliance.

#### **Princípios básicos de conduta a serem observados:**

- Princípios de Conduta Corporativa com os nossos clientes;
- Zelar pela confidencialidade e organização das informações e documentos;
- Prezar pela transparência e honestidade na prestação de serviços de qualquer natureza;
- Alertar claramente quanto aos riscos inerentes de cada produto ou serviço prestado;
- Evitar situações que gerem conflitos de interesse ou que apenas aparentem a existência destes;
- Conhecer os clientes adequadamente através do relacionamento e da obtenção de documentos, dados e informações;
- Prestar serviços e informações de forma equânime;
- Tratar adequadamente eventuais sugestões, elogios, reclamações e críticas;
- Divulgar informações de forma clara e objetiva;
- Prestar atendimento cordial, ágil e eficaz;
- Recusar compensações, presentes e vantagens pessoais, exceto expressamente permitidos nos termos deste Código e políticas relacionadas ao tema;

#### **5. Controles Internos:**

A System Manager por ser uma empresa consolidada possui um controle interno dentro dos parâmetros inerentes e muito importante dentro e fora do seu campo de atuação, ela possui uma das tarefas mais importantes dentro do universo corporativo, uma vez que esse controle atua como uma espécie de “armadura protetora” para a organização, protegendo-a de riscos que possam comprometer seu funcionamento administrativo.

Esse tipo de controle a ações como controle de segurança, instalação de câmeras e outras ações preventivas, especialmente quando pensamos no aspecto físico de uma empresa.

Entretanto, em geral, esse conjunto de estratégias contribui para muito além dos âmbitos físicos.

A criação de regras para a minimização de riscos é uma medida muito importante dentro da empresa, pois as regras ajudam desde a manutenção do fluxo de dentro da empresa, pois as regras ajudam desde a manutenção do fluxo de operações da empresa, através de medidas que vão da proteção dos dados financeiros ao gerenciamento da organização, até o estabelecimento de processo para a empresa lidar com o recebimento e a geração de relatórios financeiros e administrativos, mantendo suas finanças e o setor corporativo sempre saudáveis e sempre obtendo ótimos resultados.

De forma geral, nosso controle interno são mecanismos, regras e procedimentos implementados por nossa empresa para garantir a integridade das informações financeiras e contábeis da companhia.

Além de cumprir as leis e regulamentos, o controle interno da empresa ajuda na melhoria da eficiência operacional do empreendimento como um todo.

Os procedimentos ou políticas implementadas pela administração para o controle interno contemplam, entre outros objetivos:

- Proteger ativos;
- Estabelecer responsabilidades;
- Aumentar a eficiência;
- Estabelecer procedimentos;
- Impedir comportamentos fraudulentos;
- Otimizar operações.

A importância atribuída ao nosso controle interno aparece em todos os níveis da nossa organização. A execução de medidas sistemáticas garante, por exemplo, e que as transações comerciais ocorram de acordo com a autorização geral e específica da administração.

A System Manager através do nosso controle interno em uma organização é aquele que garante a melhor utilização possível dos recursos da empresa, ajudando, assim, a mitigar o risco envolvido com mau uso dos ativos e outros recursos da organização.

A companhia possui um alto nível de confiança em seus colaboradores, ainda assim é necessário ter um sistema de controle interno, independente do porte da empresa.

No caso da fraude financeira, as repercussões podem afetar toda a reputação da empresa, mesmo que apenas uma pessoa tenha sido autora.



Embora cada empresa possa estabelecer os seus próprios sistemas de controle interno, nossa companhia busca sempre com excelência trazer todos os itens de nosso controle.

## **6. Política da Empresa:**

A System Manager possui sua rotina e procedimentos para que todo colaborador, clientes e fornecedores possam usufruir um ambiente saudável e produtivo para atender todos os requisitos legais e sempre visando a eficiência para que se tenha um ambiente de trabalho mais seguro e de ótima convivência.

## **7. Gerenciamento de Risco Operacional**

### **Em Implantação: Previsão Maio/25**

Gestores e Colaboradores:

Identificar os riscos operacionais oriundos do exercício de suas atividades, considerando também todos os serviços;

Estabelecer e gerenciar os controles de risco inerentes as suas atividades do dia a dia.

Avaliar regularmente o serviço pactuado com colaboradores e prestadores de

Serviços;

Informar à Diretoria os eventos de risco operacional;

Monitoramento que deve possuir um ambiente interno propício para a prática de controles internos e gestão de riscos onde os objetivos estratégicos sejam fixados, os eventos de risco identificados e avaliados, uma resposta para a ocorrência dos riscos mapeados deve ser estabelecida.

Deve haver atividades de controle, um fluxo de informações e comunicações na empresa e por fim, um monitoramento contínuo dos riscos relevantes.

Assessorar a Alta Administração no desempenho de suas atribuições relacionadas à adoção de estratégias, políticas e medidas voltadas à disseminação da cultura, mitigação de riscos e da conformidade com as normas aplicáveis;

Estabelecer diretrizes para garantir o cumprimento à regulamentação vigente, inibir riscos incompatíveis ou desnecessários, aumentar a eficácia das áreas de negócios, melhorar a efetividade dos controles e minimizar o impacto aos riscos a que estão sujeitos.

Disseminar à instituição, em seus diversos níveis, o risco documentado, bem como o procedimento para reporte de ocorrência relacionadas a não observância dos níveis de riscos.

## **8. Controles Administrativos:**

Os controles administrativos da System Manager, engloba setores como análises estatísticas de lucratividade por linha de produtos e serviços, análise das variações entre valores orçados e efetivados, dentre outros.

Assim esse tipo de controle interno pode ajudar a empresa a manter suas informações organizadas, assim como o seu gerenciamento.

Os dados organizados podem aumentar a produtividade e preparar melhor o empreendimento para negociações e transações, assim como facilitar processos de revisões ou auditorias de conformidade que sejam obrigatórias de tempos em tempos.

## **9. Controles Contábeis:**

Como parte dos controles internos contábeis, temos: domínio de sistemas de conferências, orçamento, aprovações e autorizações financeiras, controles sobre ativos, auditoria interna e uma governança corporativa colaborativa que trabalha conjuntamente com área de Compliance para trazer cada vez mais melhorias e avanço em nossas operações e também estabelecer controles contábeis que pode ajudar a empresa a prevenir ou reduzir fraudes.

Nosso controle interno inclui atividades como reconciliar extratos bancários e revisões de auditoria interna, que podem descobrir se o dinheiro da empresa está sendo utilizado para os seus devidos fins.

## **10. Controles de gestão do Recursos Humanos:**

Dentre as áreas contempladas pelo controle interno estão os processos de seleção e recrutamento de novos funcionários, treinamento de equipes, supervisão, entre outros;

Aqui é possível estabelecer controles internos que podem ajudar a empresa a reduzir erros, o que gera economia para o empreendimento.

O treinamento de funcionários é um exemplo que nossa companhia usa dentro de um cotidiano claro de controle interno que pode reduzir erros, um treinamento pode ir desde atividades simples, como a otimização de treinamentos específicos.

## **11. Compliance:**

A System Manager por sua vez possui um departamento de Compliance eficiente e é um determinante mecanismo de Integridade e sistema, baseia-se em pilares, os quais definem a forma como a organização irá atuar no dia a dia.

A área de compliance é responsável por monitorar as atividades de controles internos, apontando as conclusões dos testes efetuados, bem como as recomendações e relatório anual de compliance.

São linhas fortes e abrangentes sem margem para dúvidas quanto à direção a ser seguida.

Esses pilares são o efeitos do mecanismo de Integridade e Sistema de Compliance e o sucesso da sua aplicação incondicional da Alta Direção da empresa.

Nosso sistema de Compliance é um mecanismo de Integridade e de fácil entendimento e assimilação por parte de nossos colaboradores, gerando valores que o fundamentam e guiam as ações da empresa, de suas pessoas e todas as partes relacionadas.

O departamento de Compliance de nossa companhia impõe o foco na prevenção.

Todavia, é impossível prevenir a totalidade das situações e, dessa forma, detectar assume um papel fundamental.

A partir daí, a empresa precisa adotar postura consequente e corrigir imediatamente, caso algum desvio seja identificado.

Dessa forma, ficam consolidados os 3 pilares: prevenir, detectar e responder.

## **12. Código de Ética e Conduta Bem Definido:**

Desenvolver e divulgar um código de ética e conduta claro, acessível e compreensível para todos os colaboradores.

Cabe aqui ressaltar a importância do nosso Código de Conduta que é bem

elaborado, para abranger os aspectos mais relevantes da organização, suas relações, seus riscos e seus princípios.

Desta forma, configura-se como evidente a necessidade deste Mecanismo de

Integridade e Sistemas de Compliance, Treinamento e Sensibilização muito eficiente, de forma a assegurar que todos os públicos-alvo sejam abrangidos, com o objetivo de todos assimilarem o conteúdo e agirem com ética e integridade.

#### a) Prevenir:

Este é nosso pilar mais importante, é onde a nossa empresa investe continuamente a maior parte de seus recursos. É mais inteligente prevenir que remediar. Para ser eficaz na prevenção, a companhia estabelece políticas e procedimentos claros, eficaz na prevenção, a companhia estabelece políticas e procedimentos.

Dentro desse procedimento temos as seguintes etapas:

- Desenvolver e divulgar um código de ética e conduta claro, acessível e compreensível para todos os colaboradores.
- Realizar treinamentos regulares sobre ética e conduta, garantindo que todos os funcionários compreendam o código e saibam como aplicá-lo.
- Atualizar treinamentos periodicamente para refletir mudanças nas políticas ou no ambiente regulatório.
- Estabelecer canais de comunicação abertos e seguros para que os colaboradores possam esclarecer dúvidas sobre o código de ética e conduta.

#### b) Detectar

Uma organização é formada por pessoas e estas podem agir em desacordo com o Código de Conduta, transgredir normas e leis ou incorrer em desvios por diversas razões. Assim, por melhor que seja a prevenção, impossível atingir a perfeição. Por consequência, a detecção assume o papel fundamental.

#### c) Corrigir

Esse é o pilar de nossa empresa para desvios em relação ao princípio da instituição, independentemente do nível hierárquico envolvido.

Se detectada, a falha deve ser corrigida de imediato e, se aplicável, uma medida disciplinar pertinente deve ser aplicada imediatamente.

O uso inadequado desse pilar colocará todos os Mecanismos de Integridade e

Sistemas de Compliance em risco.

Credibilidade é crucial e, se ela for arranhada, todo o trabalho será perdido

Nossa companhia leva a risca todo parâmetro que seja inerente a Lei, assim temos a Lei Anticorrupção nº 12.846/13, regulamentada pelo Decreto nº 8.420/15, a necessidade de sermos referência em todos os aspectos seja ele dentro ou fora da companhia ganha uma importância como forma de competitividade e reduzir custos com ações e outros procedimentos jurídicos.

Diante desse breve histórico da expressão, fica bem mais fácil entender quando se trata de "compliance". Isso quer dizer que nossa organização possui todo um sistema de política e procedimentos cujo objetivo é impedir e prevenir atos lesivos.

É feito através da atenção ao atendimento das leis externas e criação de normas internas, como um código de ética, que deve ser seguido por todos dentro do negócio e por quem presta serviços à empresa.

No mercado atual, estar em compliance não é uma escolha, mas um dever de toda organização que pretende mostrar-se para o mercado como uma instituição séria e comprometida com a retidão dos seus colaboradores.

Para atingir esse objetivo, mais do que uma equipe comprometida, é preciso contar com parceiros que, além de dividirem os mesmos preceitos, também oferecem soluções que agilizam os processos e tornam o cumprimento do programa de integridade mais fluido no dia a dia.

Dentro desse procedimento temos as seguintes etapas:

- Manter um canal de denúncia acessível, confidencial e, preferencialmente, anônimo para que os colaboradores possam reportar desvios sem medo de retaliação.
- Promover a existência e o uso desse canal entre os funcionários.
- Implementar medidas corretivas para evitar a recorrência de desvios, como retreinamento, mudanças nos processos ou reforço dos controles internos
- Comunicar a toda a empresa sobre as ações gerais tomadas para reforçar a integridade e a importância de seguir o código de ética, sem expor detalhes específicos de casos individuais.
- Oferecer treinamentos regulares e específicos sobre ética e conduta, focados nas áreas onde os desvios foram identificados.
- Garantir que a liderança da empresa esteja ativamente envolvida no monitoramento e na correção de desvios, demonstrando compromisso com a ética e a integridade.

### **13. PROGRAMA DE GOVERNANÇA CORPORATIVA:**

Para estar em compliance não basta estar em conformidade com leis e regulamentos, sejam eles internos e externos.

É, principalmente, compreender e adotar princípios de integridade e conduta ética na cultura organizacional.

Agentes de Governança: são indivíduos e órgãos envolvidos no sistema de governança, tais como os sócios, diretores e gerentes.

Os agentes de governança têm papel relevante no fortalecimento e na disseminação do propósito, dos princípios e dos valores da organização, visto que a liderança e o comprometimento dos administradores e demais executivos são determinantes para a formação de um ambiente ético.

A Alta Administração tem a responsabilidade de explicitar de forma clara os propósitos da Companhia, garantir o foco nas necessidades, além de ajudar a estabelecer os processos necessários para concretizar esses objetivos.

Colaboradores, administradores, prestadores de serviços, estagiários, terceirizados, aprendizes e aqueles que exercem mandato, cargo, emprego ou função, ainda que transitoriamente e sem remuneração, por eleição, nomeação, convênio, contratação ou qualquer outra forma de investidura ou vínculo.

Compliance: deriva do verbo inglês “to comply”, que significa estar em conformidade, isto é, em fazer cumprir leis, decretos, regulamentos, instruções e normas aplicáveis na Companhia, e que na hipótese de não cumprimento, podem gerar sanções, perda financeira e danos à reputação ou à imagem institucional.

Ética é um conjunto de valores morais e princípios que norteiam a conduta humana na sociedade.

A ética serve para que haja um equilíbrio e bom funcionamento social.

Neste sentido, a ética, embora não possa ser confundida com as leis, está relacionada com o sentimento de justiça social e permeia basicamente todos os fatores da vida em sociedade.

Ato intencional praticado por um ou mais indivíduos entre gestores, responsáveis pela governança, empregados ou terceiros, envolvendo o uso de falsidade para obter uma vantagem injusta ou ilegal.

Integridade: deriva do termo latim “integritate”.

Refere-se à qualidade de alguém ou algo que se integre, de conduta reta.

Aquilo que é íntegro é algo que não carece de nenhuma das suas partes ou, referindo-se a uma pessoa, trata-se de alguém que é reto, honesto e exemplar.

Liderança: processo da influência que se tem sobre outras pessoas, motivando e incentivando a trabalharem com entusiasmo por um objetivo comum.

O líder deve agir de forma ética e positiva estimulando os liderados para que contribuam voluntariamente a alcançarem os objetivos da equipe e da organização.

É a aplicação prática da conduta ética e integridade institucionalizada com o objetivo de Programa de Compliance Governança Corporativa, prevenir, detectar e mitigar riscos corporativos, desvios, fraudes, irregularidades e atos ilícitos contra a administração pública ou que gerem dano ao erário.

Sistema de Governança: conjunto de práticas integradas das atividades das áreas de Gestão de Riscos, Controles Internos, Auditoria e Compliance.

## 14. LIDERANÇA ÉTICA E INTEGRIDADE:

Atuar estrategicamente em soluções de Tecnologia, por meio de Parceiros de negócios e apoio ao desenvolvimento socioeconômico, sempre pautando sua conduta na ética e na integridade.

Assegurar que todos os nossos processos e atividades estejam em conformidade com as leis e regulamentos aplicáveis e com os nossos princípios e valores;

Possibilitar que os responsáveis pela tomada de decisão, em todos os níveis, tenham acesso tempestivo a informações completas e confiáveis quanto aos riscos de nossas atividades e negócios;

Aumentar a probabilidade de alcance dos nossos objetivos estratégicos, reduzindo os riscos a níveis aceitáveis;

Criar uma cultura de conformidade, transparência, integridade e observância às regras estabelecidas na legislação;

Liderar pelo exemplo: reforçar o comportamento ético, fomentando os valores institucionais;

Incentivo à denúncia: lembrar os colaboradores sobre suas obrigações de comunicar práticas ilícitas ou antiéticas;

Mitigar a ocorrência de corrupção, fraude e desvios éticos em nosso ambiente interno e em nossas relações com terceiros;

Zelar pela nossa imagem perante a sociedade;

Contribuir para o alcance de um ambiente de negócios ético e íntegro.

Nosso Programa está alinhado com os preceitos da Lei.

Nossa história é marcada por grandes mudanças e desafios, pela expansão de nossos negócios e atividades para possibilitar o atingimento de nossa missão, sem jamais abrirmos mão da ética e da integridade.

Temos pleno entendimento de que, em um ambiente no qual as más condutas proliferam, não basta fazer o que é certo, é importante influenciar positivamente todo o ambiente de negócios e zelar pela integridade em toda a nossa rede de relacionamentos.

Com essa percepção, buscamos evoluir continuamente em nossas políticas, práticas e controles e, principalmente, no amadurecimento da nossa cultura organizacional pautada na ética e na integridade.

Nossos administradores e colaboradores assumem pleno compromisso com este Programa, sua efetiva aplicação e seu aprimoramento contínuo.

Saber ouvir: escutar e abordar questões e preocupações no momento certo;

Treinar a equipe: organizar treinamentos sobre tomadas de decisões éticas.

Reforçar a importância do comportamento ético em todos os discursos e mensagens;

Encorajar a participação: envolver os colaboradores no processo de tomada de decisão.

O compromisso da System Manager com a implementação do Programa de Compliance visa, além de consolidar a missão, visão e valores institucionais, combater condutas antiéticas ou corruptas, protegendo a reputação da empresa e suas ações.

Ademais, fomentar a perenidade da Companhia no mercado.

#### **15. Diretrizes de Conformidade:**

Na System Manager a conformidade deve ser observada por todos os colaboradores devendo ser um norteador de todas as condutas individuais e coletivas.

Buscando garantir a conformidade com os requisitos legais, regulatórios, autorregulatórios e normativos internos, sendo responsável pelos aspectos de governança, conduta e transparência, gerando uma cultura organizacional de valorização da ética e da integridade, as diretrizes de conformidade compreendem:

Zelar pela implantação, execução, cumprimento e observância dos normativos externos e internos, das recomendações dos órgãos de supervisão e da autorregulação;

Difundir elevados padrões de integridade e conduta, através da disseminação da cultura de conformidade, em observância aos princípios e às diretrizes estabelecidas no Código de Conduta.

Assegurar uma gestão independente e autônoma, garantindo a isenção e imparcialidade na atuação da função de conformidade, bem como ter pleno acesso às informações necessárias para a execução das atribuições;

Assegurar a confidencialidade no desempenho das atribuições relativas à função de conformidade;

Garantir livre e imediato acesso dos responsáveis pela função de conformidade ao Conselho de Administração, à Diretoria Executiva, ao Comitê



de Auditoria, quando constituído, e aos órgãos regulamentares e fiscalizadores, visando o gerenciamento efetivo do risco de conformidade;

Disponer de recursos compatíveis e suficientes para o desempenho eficaz da função de conformidade, inclusive em relação à alocação de pessoal em quantidade suficiente, adequadamente capacitado e com a experiência necessária para o exercício das atividades;

Prover capacitação para todos os colaboradores sobre conformidade;

Prevenir danos à reputação e inibir atos ilícitos, mantendo a confiança das partes interessadas, associados ou clientes, colaboradores e da sociedade;

Zelar pela efetividade das medidas corretivas tomadas quando inconformidades forem identificadas;

Zelar e orientar sobre as boas práticas de governança e de conduta.

## **16. Due Diligence**

### **Em implantação: Agosto/2025**

Esta ferramenta é eficaz na mitigação dos riscos uma vez que busca o conhecimento do histórico de um terceiro antes mesmo da negociação.

O monitoramento e tratamento dos riscos advindos de parceiros comerciais é importante, pois se o contratado cometer algum ato de corrupção, ambas poderão ser legalmente responsabilizadas.

As informações devem conter o histórico de envolvimento em casos de corrupção, fraudes, processos judiciais, entre outros, no setor em que atua;

Programa de Due Diligence: mapeamento dos riscos que a Companhia está submetida, incluindo os riscos de compliance.

Indicadores de Due Diligence: permitem acompanhar e avaliar de forma periódica a gestão da empresa em todos os aspectos.

Esses indicadores podem ser, mas não se limitando a quantidade de servidores e partes interessadas capacitadas em conscientização antifraude e anticorrupção, a quantidade de áreas submetidas a gestão de risco; a quantidade de riscos identificados e sua gravidade; a quantidade de riscos mitigados; a quantidade de riscos residuais; as Comunicações realizadas; a Quantidade de notícia negativa na mídia; a quantidade de medidas disciplinares instauradas; a quantidade de esquemas fraudulentos e corruptos conhecidos e cometidos contra a organização; a quantidade e natureza das denúncias recebidas no Canal de Ética; a quantidade e natureza de fraude e corrupção

apuradas, confirmadas e sanadas; a Recorrência da fraude e corrupção; a quantidade de investigações em fraude e corrupção; a estimativa de perdas ocorridas com a fraude e corrupção.

Treinamentos: capacitação e conscientização contínua de todos os colaboradores e parceiros nas atividades e práticas do Programa de Compliance.

Para sucesso da aplicação do Programa de Due Diligence na Companhia não basta que exista um setor responsável por Governança e Compliance.

É necessária uma abordagem coordenada, dinâmica e de forma sistemática, mitigando eventuais lacunas para a total eficácia do Programa.

Todos os colaboradores da System Manager são responsáveis pela aplicação do Programa de Compliance em suas rotinas. Sendo assim, devem:

Apresentar as informações solicitadas, de forma oportuna e completa;

Cumprir as leis e os normativos internos, como o Código de Conduta Ética e Integridade;

Monitorar as operações e estar atento às mudanças nas leis e regulamentos que afetem suas atividades;

Envolver-se nas ações de Compliance, na medida de suas responsabilidades;

Assumir a responsabilidade pela mitigação dos riscos identificados na sua área;

Implementar controles propostos e propor melhorias;

Denunciar qualquer ato ilícito ou desvio ético de que tenha conhecimento nos canais dispostos na Companhia;

Disseminar a cultura de controles internos e Compliance e divulgar o Programa aos demais colaboradores.

Neste sentido, todos são agentes de compliance e, portanto, devem agir em conformidade com as leis e regulamentos aplicáveis ao escopo das atribuições.

Em caso de eventuais dúvidas ou dificuldades quanto ao Programa de Compliance os empregados devem procurar seus gestores ou comunicar a Assessoria de Governança Corporativa e de Compliance.

A System Manager por sua vez possui um departamento de Compliance eficiente e é um determinante mecanismo de Integridade e sistema, baseia-se em pilares, os quais definem a forma como a organização irá atuar no dia a dia.

São linhas mestras simples, fortes e abrangentes sem margem para dúvidas quanto à direção a ser seguida. Esses pilares são os esteios do Mecanismo de Integridade e Sistema de Compliance e o sucesso da sua aplicação incondicional da Alta Direção da empresa.

Nosso sistema de Compliance é um mecanismo de Integridade e de fácil entendimento e assimilação por parte de nossos colaboradores, gerando valores que o fundamentam e guiam as ações da empresa, de suas pessoas e todas as partes relacionadas.

## **17. NORMAS DE CONDUTA**

No exercício de suas funções, o colaborador deve agir com a mesma atitude que qualquer pessoa honrada e de caráter íntegro agiria na relação com outras pessoas na administração dos seus próprios negócios.

O colaborador deve atuar sempre em defesa dos melhores interesses da System Manager, mantendo confidencialidade sobre os negócios e operações da empresa.

É fundamental que as atitudes e comportamentos do colaborador reflitam sua integridade pessoal e profissional, e não coloquem em risco sua própria segurança financeira e patrimonial ou a da System Manager.

Avaliar criteriosamente situações que possam caracterizar conflito entre seus interesses e os da System Manager, ou condutas que possam não ser aceitáveis do ponto de vista ético, mesmo que não causem prejuízos tangíveis à System Manager.

## **18. CONDUTAS REPROVÁVEIS**

Valer-se do cargo, função ou informações sobre negócios e assuntos da System Manager ou dos clientes da empresa, para influenciar decisões que venham a favorecer interesses próprios ou de terceiros;

Aceitar ou oferecer, direta ou indiretamente, favores ou outros benefícios de caráter pessoal que resultem de relacionamento com a System Manager e que possam influenciar decisões, facilitar negócios ou beneficiar terceiros. Presentes não enquadrados nessa situação devem ser informados a Diretoria da empresa.

Indicar a contratação de parentes ou levar outra pessoa a indicá-los, sem informar o influenciar decisões, facilitar negócios ou beneficiar terceiros. Presentes não enquadrados nessa situação devem ser informados a Diretoria da empresa.

Indicar a contratação de parentes ou levar outra pessoa a indicá-los, sem informar o fato a Diretoria;

Usar equipamentos e outros recursos da System Manager para fins particulares não autorizados;

Envolver-se em atividades particulares, não autorizadas, que interfiram no tempo de trabalho dedicado à System Manager;

Usar para fins particulares, ou repassar a terceiros, tecnologias, metodologias,

conhecimentos ou informações de propriedade da System Manager, ou por ela

desenvolvidas ou obtidas;

Manifestar-se em nome da System Manager, quando não autorizado a fazê-lo oficialmente.

## **19. CONDUTAS ESPERADAS**

Reconhecer os erros cometidos e comunicá-los imediatamente a Diretoria;

Não cumprir as orientações que vão contra os princípios e valores da System Manager;

Atuar de modo a melhorar a integração entre os funcionários com os quais se relaciona diretamente ou não;

Apresentar críticas construtivas e sugestões, visando a aprimorar a qualidade e ambiente de trabalho.

## **20. RELACIONAMENTO COM AS PARTES INTERESSADAS**

Todas as pessoas que se relacionam ou sofrem influência com os atos e decisões da System Manager).

O compromisso com a satisfação das partes interessadas deve refletir-se no respeito aos seus direitos e na busca por soluções que atendam a seus interesses, sempre em acordo com os objetivos de desenvolvimento da System Manager.

## **21. DIRIGENTES**

O relacionamento com diretores da System Manager e outras entidades devem basear-se na comunicação precisa, transparente e no momento correto com informações que lhes permitam acompanhar as atividades e o desempenho da System Manager, bem como na busca por resultados que tragam impactos positivos para todos.

Proteger as informações ainda não divulgadas publicamente e que possam afetar ou influenciar as movimentações do mercado e decisões de investimentos.

## **22. COLABORADORES**

As relações no ambiente de trabalho devem se basear pela cortesia e respeito. Colaborar para que predomine o espírito de equipe, a lealdade, a confiança, a conduta compatível com os valores da System Manager em busca de resultados.

Quando estiver no papel de supervisor de pessoas, tenha em mente que seus colaboradores o tomarão como exemplo. Suas ações, assim, devem constituir modelo de conduta para sua equipe. Não se admite o uso do cargo para solicitar favores ou serviços pessoais a subordinados.

É fundamental reconhecer o mérito de cada um e propiciar igualdade de acesso às oportunidades de desenvolvimento profissional existente, segundo as características, competências e contribuições de cada colaborador.

Não se admite nenhuma decisão que afete a carreira profissional de subordinados baseada apenas em relacionamento pessoal.

Ao exercer cargos de liderança, os supervisores darão a devida atenção e consideração aos interesses de seus colaboradores, de modo a criar um ambiente de trabalho estimulante, produtivo e agradável.

## **23. FORNECEDORES**

A escolha e contratação de fornecedores devem ser baseadas em critérios técnicos, profissionais, éticos e nas necessidades da System Manager, devendo ser conduzidas por meio de processos predeterminados, com concorrência ou cotação de preços, que garantam a melhor relação de preço e resultados econômicos.

Ser imparcial e justo nas celebrações, prorrogações, revogações ou rescisões de contratos;

Disponibilizar informações, instalações ou recursos necessários que permitam a execução dos serviços contratados com a devida qualidade;

Zelar pela confidencialidade das informações;

Monitorar e avaliar os serviços prestados com critérios bem fundamentados;

Não receber ou oferecer compensações, presentes ou vantagens diversas como contraprestação pelo serviço contratado; e apoiar ações que promovam o desenvolvimento e o bem-estar de todos.

## **24. CONCORRENTES**

A ética deve ser o elemento básico em todas as nossas operações e relações com outras empresas e instituições do mercado de informações comerciais,

Não devem ser feitos comentários que possam afetar a imagem dos concorrentes ou contribuir para a divulgação de boatos sobre eles.

Tratar as demais empresas com o mesmo respeito que a System Manager espera ser tratada.

É proibido fornecer qualquer informação, não autorizada, de propriedade da System Manager aos concorrentes.

Sempre defender a existência de um mercado competitivo, livre, justo e sustentável.

Nunca firmar acordos com competidores que eliminem ou restrinjam indevidamente a concorrência.

## **25. DO JURÍDICO:**

Identificar e mitigar o risco legal na elaboração dos contratos firmados pela instituição;

Incluir nos contratos firmados pela instituição cláusulas que estabeleçam claramente os papéis e as responsabilidades dos prestadores de serviços terceirizados e fornecedores.

Garantir a inclusão das cláusulas necessárias nos contratos.

## **26. COM OS ÓRGÃOS REGULADORES, FISCALIZADORES E GOVERNO:**

A System Manager por ser uma empresa que participa ativamente, de licitações públicas preza pela excelência e aprimoramento dos procedimentos adequados ao setor, como cumprimento de todos os seus deveres éticos, fiscais e tributários dentro da Lei de Licitações.

Negociar direta ou indiretamente com o setor público ou com outros órgãos governamentais nem sempre é o mesmo que negociar com outros tipos de empresa.

Órgãos governamentais podem ter regras diferentes daquelas observadas nas empresas privadas. Algumas práticas aceitáveis no setor privado talvez causem problemas quando a negociação se dá com empresas do governo.

A empresa conta com especialistas que podem ajudar você nessas atividades.

Não tolerar a violação de leis ou regulamentos na condução de nossos negócios;

Disponibilizar informações e documentos, quando solicitado por tais órgãos, sendo absolutamente transparente quanto aos seus atos;

Respeitar leis, regulamentos e normas vigentes;

Manter todas as informações exigidas em arquivos de forma organizada e segura;

Não inutilizar documentos e informações que possam ser importantes para o cumprimento de obrigações legais e administrativas, confidenciais ou não;

- Cumprir com os prazos;
  - Prestar somente informações fidedignas;
  - Contribuir com sugestões técnicas;
  - Cooperar plena e tempestivamente em quaisquer casos; e
- Adotar efetivos mecanismos de controles internos.

## **27. PÚBLICO, SOCIEDADE E COMUNIDADE**

A nossa conduta no relacionamento com o público, comunidade e sociedade devem refletir o respeito aos seus direitos. A System Manager deve agir sempre dentro da ética e da cordialidade.

Apoiar, sempre que possível, as realizações de eventos cívicos, culturais e sociais.

## **28. PARCEIROS**

A System Manager poderá formalizar parcerias visando os interesses comerciais, respeitando os princípios gerais declarados no item quatro deste Código de Ética.

## 29. POLÍTICAS DE TREINAMENTO:

A System Manager 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, em razão de ser fundamental que todos tenham sempre conhecimento atualizado dos seus princípios éticos, das leis e normas.

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

Neste sentido, a Empresa adota um programa de treinamento anual dos seus Colaboradores, à medida que as normas, princípios, conceitos e valores contidos neste Manual e demais políticas sejam atualizadas, com o objetivo de fazer com que eles estejam sempre atualizados, estando todos obrigados a participar de tais programas de treinamento.

A implementação do processo de treinamento e educação continuada fica sob a responsabilidade de cada área de atuação, e exige o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação.

O programa de treinamento inicial quanto o programa de reciclagem deverão abordar as atividades da Companhia, seus princípios éticos e de conduta, as normas de compliance, as políticas de segregação, quando for o caso, e as demais políticas descritas nesta Manual, 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.

Deverá ser estabelecido um programa de conscientização de segurança; treinar os colaboradores sobre temas como, mas não se limitando as melhores práticas de segurança da informação, Lavagem de dinheiro, suborno e tratamento de dados, causas de exposição não intencional de dados, reconhecimento e comunicação de vulnerabilidades e incidentes de segurança, perigos ao conectar e transmitir dados da empresa em redes não seguras; treinar as competências e conscientização de segurança para funções específicas como gestores e profissionais de tecnologia, em conformidade com a Política de Segurança da Informação e Segurança Cibernética da Companhia.

A periodicidade de cada programa de treinamento fica a critério do Gestor de cada área que designa seus colaboradores para a implementação de cada projeto de treinamento.



## **30. LEI GERAL DE PROTEÇÃO DE DADOS:**

**Em Implantação:** Data de Finalização: Jun/2025

O Comitê de Proteção de Dados Pessoais e o Encarregado de Dados Pessoais são os responsáveis pelo zelo no cumprimento desta normativa, necessária para cumprir com o que estabelece a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018 (“LGPD”).

Autoridade Nacional de Proteção de Dados ou ANPD: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus Dados Pessoais para uma finalidade determinada;

Controlador de Dados: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de Dados Pessoais;

Dado Anonimizado: dado relativo ao titular que não permita a sua identificação pela utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Dado Pessoal: informação relacionada a pessoa natural que permita de qualquer forma a identificar;

a) Dado Pessoal Sensível: Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;

b) Encarregado de Dados: pessoa indicada pelo Controlador de Dados e pelo Operador de Dados para atuar como canal de comunicação com os Titulares dos Dados e com a Autoridade Nacional de Proteção de Dados (ANPD);

c) LGPD: Lei Geral de Proteção de Dados Pessoais (Lei 13.709/18);

d) Operador de Dados: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do Controlador;

e) Titular de Dados: a pessoa natural a quem se referem os Dados Pessoais que são objeto de tratamento;

f) Tratamento de Dados ou Tratamento: toda operação realizada com Dados Pessoais, incluindo Dados Pessoais Sensíveis, como as que se referem a: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de Dados Pessoais.

## **31. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

**Em implantação: Maio/2025**

A empresa System Manager por ser uma empresa de Serviços de Tecnologia zela pelo maior pilar existente dentro da Segurança da Informação, pois agimos com efetividade neste setor que abrange serviços e software, assim buscamos não somente a excelência de nossa empresa, mais também através de nossa atuação estamos entre as empresas mais eficientes e seguras quando o aspecto é segurança da informação.

Atuamos no setor público e privado das organizações com ética e seriedade, pois não somente zelamos pela segurança de informação de nossos clientes, mais também para nossos colaboradores e fornecedores.

Em aspecto global a System Manager atinge o maior nível de excelência quando se fala em segurança da informação, sua atuação é ampla dentro dos setores governamentais e privados em grandes instituições e segmentos, pois assim nossa segurança é a de nossos clientes, pensamos a longo prazo trazer sempre comodidade e transparência em todos os nossos projetos organizacionais.

Temos certificações que nos assegura esta eficiência, pois o conhecimento e profissionalismo nos trás no aspecto de segurança da informação um viés exato de acertos e dinâmica, assim sempre buscamos investir e qualificar nossos profissionais buscando com foco na eficiência.

A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

São propriedades básicas da segurança da informação: confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Estamos em conformidade com a nova Lei Geral de Proteção de Dados, Lei: nº 13.709/2018, assim trazendo mais segurança determinante para nossos clientes.

Segurança da informação é a prática que mantém os dados em sigilo, a defesa do que não é público, nossa metodologia de segurança nos permite a atingir o maior grau de proteção de dados e outras informações relevantes.

A segurança da informação é aquele conceito por trás da defesa dos dados, detalhes e afins para assegurar que eles estejam acessíveis somente aos seus responsáveis de direito ou as pessoas às quais foram enviados, por isso tomamos todas as precauções de segurança.

Se o compartilhamento de informações com fornecedores e clientes externos não for considerado ilegal nem contrário à prática empresarial ou comercial, a companhia incentivar esse compartilhamento quando ele puder melhorar a qualidade ou a utilização dos produtos e serviços.

Se for necessário divulgar informações de propriedade da companhia para pessoas fora da empresa, prepare um acordo escrito de confidencialidade e não divulgação, e estabeleça controles adequados para administrar o fluxo de informações.

Garantir que todos os meios de processamento e ou conservação de informação contenham medidas de proteção quanto ao acesso e utilização por pessoa não autorizada, assegurando com isso que toda informação esteja protegida de revelações acidentais, espionagem industrial, violação da privacidade e outras ações similares.

Assegurar que toda informação processada em cada um dos sistemas de informação e processos transacionais seja necessária, útil e suficiente para o desenvolvimento dos negócios. Esteja livre de erros ou irregularidades, de qualquer espécie.

Garantir que a informação e sua capacidade de processamento, manual e automática, sejam resguardadas e recuperadas sempre que necessário, de modo a não impactar significativamente o andamento dos negócios.

Assegurar que toda informação e os meios físicos que a contenham, processem e ou transportem, cumpram com os regulamentos legais vigentes em cada âmbito, e que todos os direitos de propriedade sobre a informação utilizada ou produzida pela System Manager, no desenvolvimento de suas atividades, estejam adequadamente estabelecidos a favor da empresa.

A System Manager tem os seguintes princípios gerais de segurança da informação:

a) Preservar e proteger as informações e os recursos de informação da System Manager ou de terceiros, ou que estejam sob sua responsabilidade, dos diversos tipos de ameaça e em todo o seu ciclo de vida, contidas em qualquer suporte ou formato;

b) Prevenir, monitorar, identificar e responder aos incidentes de segurança da informação, reduzindo os seus impactos e assegurando a confidencialidade, integridade, disponibilidade, autenticidade das informações e a conformidade no uso dos recursos de informação no desenvolvimento das atividades profissionais;

c) Cumprir a legislação vigente no Brasil e demais instrumentos regulamentares relacionados ao negócio no que diz respeito à segurança da informação e aos objetivos corporativos, morais e éticos da System Manager.

As medidas de prevenção e controle adotadas pela System Manager visam, em essência, gerenciar e manter os riscos em um nível adequado ao negócio.

A System Manager, por meio de seus programas individuais, contribui coletivamente para o Programa de Segurança da Informação.

Os programas são documentados e atualizados anualmente para garantir a conformidade contínua com os requisitos regulamentares

2. Ela exige que tais instituições desenvolvam, implementem e mantenham uma política de Segurança Cibernética abrangente baseada em princípios e diretrizes que buscam garantir a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados. A política de segurança cibernética deve abranger:

### **32. Propriedade intelectual:**

A System Manager valoriza informações sobre novos serviços, produtos, ideias comerciais, conceitos e outras informações geradas na empresa.

Protegendo os direitos de propriedade intelectual da companhia, evitando a divulgação imprópria ou não autorizada, contra o uso ilegal ou indevido, identificando-a com o logotipo, a logomarca ou a advertência de direito autoral ou patente pertinente.

A System Manager respeita e honra os direitos de propriedade intelectual de terceiros. Não usaremos direitos patenteados por terceiros sem antes obter licença ou aprovação do departamento jurídico da System Manager.

### **33. Direitos autorais:**

Diversos materiais utilizados no decorrer de nosso trabalho são protegidos por leis de direito autoral.

Não é permitido reproduzir, distribuir ou alterar materiais de terceiros cujos direitos autorais estejam protegidos por lei, exceto mediante autorização prévia. Exemplos de materiais comumente protegidos pela lei de direitos autorais: Software

### **34. POLÍTICA DE SUSTENTABILIDADE:**

A System Manager deve sempre buscar adotar práticas e ações sustentáveis para minimizar eventuais impactos ambientais, incluindo, mas não se limitando a:

- I. utilização de papel reciclável para impressão de documentos;
- II. utilização de refil de cartuchos e toners para impressão;
- III. separação do material reciclável para fins de coleta seletiva de lixo;
- IV. utilização de lâmpadas de baixo consumo energético;

V. incentivo à utilização de meios de transporte alternativos ou de menor impacto ambiental por seus Prestadores de Serviço, como transportes coletivos, caronas ou bicicletas. Além disso, a Empresa incentiva seus Prestadores de Serviço a adotarem postura semelhante no dia a dia de suas atividades, por exemplo:

- I. evitar imprimir e-mails e arquivos eletrônicos, exceto se necessário;
- II. optar por utilizar canecas ou copos reutilizáveis;
- III. desligar os computadores todos os dias ao final do expediente;
- IV. apagar as luzes das salas ao sair; e
- V. desligar as torneiras de pias de cozinha e banheiros quando não estiver fazendo uso.

### **35. GESTÃO DO CÓDIGO DE ÉTICA**

A gestão do Código de Ética cabe a Diretoria.

Nossa área de compliance é responsável por sua divulgação e observância de sua aplicação.

Compete a cada colaborador cumprir e zelar para que sejam respeitados os princípios éticos previstos neste Código de Ética.

### **36. Missão, Visão e Valores da System Manager:**

- Missão:  
Simplificamos a tecnologia para empreendedores e os ajudamos a controlar e crescer seus negócios.
- Visão:

Construir a próxima geração de serviços de tecnologia para empreendedores.

- Valores:  
Falamos a verdade;  
Somos humildes;  
Buscamos a inovação sempre, sem medo de errar;  
Gostamos de trabalhar, ainda mais em equipe;  
Cultivamos relações informais e descontraídas.

### **37. POLÍTICA ANTI - CORRUPÇÃO E SUBORNO**

A System Manager valoriza a honestidade, transparência e respeito em todas as suas relações.

Portanto, não permite e não incentiva em nenhuma hipótese a obtenção de vantagem de forma ilícita.

A Lei Anticorrupção, obrigatoriamente, devem ser cumpridas.

Caso a conformidade com esta Política implique na violação dessas leis em algum aspecto, as leis devem ser seguidas, devendo ser previamente informada sobre o conflito para o devido tratamento e providências.

Com base nesses princípios, a System Manager e seus respectivos colaboradores devem observar as diretrizes constantes no nosso Código de Conduta, além de pautar a condução dos negócios de maneira honesta, responsável, ética, transparente, profissional e com a observância das leis.

A System Manager preza por práticas de negócios justas e economicamente sustentáveis.

Assim como os indicadores econômicos, a percepção pública é um indicador do sucesso de nossa Companhia.

Essencialmente: a reputação da Companhia é o nosso maior patrimônio.

E, assim sendo, precisa ser protegida, conforme detalhado abaixo, esta Política tem o intuito de auxiliar o colaborador a compreender as obrigações, premissas e normas da Lei Anticorrupção e como elas impactam nos negócios realizados pela Companhia.

Adicionalmente, este material também traz as diretrizes relacionadas a conduta da Companhia e sua Política Anticorrupção.

Quaisquer ações não previstas nesta Política e que estejam relacionadas aos temas aqui abordados, desde que não resultem em descumprimento de

aspectos legais e regulatórios vigentes, deverão ser submetidas à avaliação prévia de uma comissão composta por membros da Administração e Departamento Jurídico.

Uma lei ordinária de autoria do Poder Executivo Federal que trata da responsabilização objetiva administrativa e civil de empresas pela prática de atos contra a Administração Pública, nacional ou estrangeira.

No mesmo sentido da Lei Anticorrupção, a qual define uma série de exigências que também devem ser obedecidas pela Companhia, seus administradores, diretoria e conselho, colaboradores e terceiros.

Assim como a Lei Anticorrupção Brasileira, prevê a aplicação de sanções cíveis, administrativas e penais para casos que atentarem contra a lei.

Esta Política foi elaborada com o objetivo de esclarecer aos colaboradores o conteúdo, alcance e disposições das Leis, bem como promover a conscientização

sobre a importância e responsabilidade dos atos praticados em nome da System Manager, reafirmando o compromisso com a transparência e integridade na condução do nosso negócio.

A Lei Anticorrupção permite que as empresas sejam punidas e responsabilizadas por atos de seus colaboradores, em qualquer nível hierárquico, praticados contra a Administração Pública nacional ou estrangeira (União, Estados, Municípios, órgãos públicos, etc.).

Além da penalização das empresas, os colaboradores envolvidos em atos lesivos à Administração Pública também são passíveis de serem responsabilizados administrativamente, civil e criminalmente, podendo ser dispensados por justa causa, indenizar todos os prejuízos financeiros sofridos pela empresa, respondendo por processo criminal.

O colaborador que possuir qualquer dúvida sobre o conteúdo explícito nesta Política ou sobre a Lei Anticorrupção (Lei nº 12.846/13), deverá prontamente solicitar esclarecimentos ao seu gestor imediato.

Caso necessário, cabe à busca de apoio junto ao Departamento Jurídico ou até mesmo advogados externos para os esclarecimentos.

A Política Anticorrupção está disponível para consulta nos sites institucionais da Companhia.



Conhecida como “Lei Anticorrupção”, (“Lei 12.846/13” ou “Lei Anticorrupção”), a qual busca combater e prevenir atos de corrupção.

Esta Política aplica-se à System Manager e à todos seus escritórios pelo Brasil e unidades de negócio, com o dever de ser observada e considerada por todos os colaboradores, incluindo administradores, diretoria, conselho e qualquer terceiro com os quais mantenha relacionamento contratual.

A System Manager, tem o dever de divulgar e comunicar o conteúdo desta Política a todos os colaboradores da Companhia, parceiros e pessoas ligadas a empresa, assim valorizando a honestidade, transparência e respeito em todas as suas relações, portanto não incentiva em nenhuma hipótese a obtenção de vantagem de forma ilícita.

Caso a conformidade com esta Política implique na violação dessas leis em algum aspecto, as leis devem ser seguidas, devendo ser previamente informada sobre o conflito para o devido tratamento e providências.

Com base nesses princípios, a System Manager e seus respectivos colaboradores devem observar as diretrizes constantes no nosso Código de Conduta, além de pautar a condução dos negócios de maneira honesta, responsável, ética, transparente, profissional e com a observância das leis.

E, assim sendo, precisa ser protegida, conforme detalhado abaixo, esta Política tem o intuito de auxiliar o colaborador a compreender as obrigações, premissas e normas da Lei Anticorrupção e como elas impactam nos negócios realizados pela Companhia.

As leis de corrupção e suborno a quais a System Manager opera proíbem o suborno. Por exemplo, a Lei de Práticas de Corrupção Estrangeira dos Estados Unidos (“FCPA – U.S.Foreign Corrupt Practices Act”) e a Lei Antissuborno do Reino Unido (“UK Anti-Bribery Act”) proíbe suborno a oficiais do governo e outros oficiais (tais como candidatos políticos, partidos políticos e seus oficiais, empregados de negócios governamentais, oficiais das Nações Unidas, etc.).

A Lei Antissuborno do Reino Unido também proíbe subornos a parceiros comerciais. Tanto a FCPA quanto a Lei Antissuborno do Reino Unido se aplicam às atividades que aconteçam em qualquer lugar do mundo. Uma violação poderá ser uma ofensa criminal grave para todos os envolvidos. Uma violação pode resultar em multas e penalidades para a empresa, assim como multas, penalidades e prisão para os indivíduos.

Não é aceitável sob qualquer circunstância que qualquer parceiro comercial ofereça ou dê qualquer coisa de valor, direta ou indiretamente, a qualquer contraparte comercial (incluindo a seus funcionários e diretores), oficiais do governo, contratados e subcontratados do governo, candidatos políticos ou partidos políticos, em seu país natal ou em qualquer outro local, para obter ou manter negócios ou para obter qualquer vantagem de qualquer tipo.



Parceiros de negócios proibirão qualquer pagamento oferecido indevidamente, fornecido para influenciar ou induzir qualquer ato ou decisão de oficiais do governo (de qualquer nível do governo) ou para garantir qualquer vantagem indevida.

Parceiros de negócios não farão qualquer pagamento diretamente para oficiais do governo ou por meio de um terceiro com o conhecimento de que o pagamento será dado a um oficial do governo em troca de uma ação favorável em nome da Smanager, ou do parceiro de negócios.

Sob as leis antissuborno, a Smanager, seus empregados e seus parceiros comerciais também estão proibidos de fazer indiretamente o que estão proibidos de fazer de forma direta – não faça qualquer pagamento a um terceiro se o todo ou parte do pagamento for destinado a uma pessoa para uma finalidade proibida.

### **38. Conceitos e Aplicação das Leis Anticorrupção(12.846/13).**

#### **a) Corrupção:**

É todo ato lesivo à Administração Pública, nacional ou estrangeira, que atente contra o patrimônio público, contra princípios da administração pública ou contra os compromissos internacionais assumidos pelo Brasil.

#### **b) Ato Lesivo:**

É a ação do indivíduo ou da Companhia que causa prejuízo.  
Para fins de aplicação desta Lei, o ato lesivo é ilícito, ou seja, contrário a Lei.

#### **c) Suborno:**

Consiste na promessa, oferta, doação ou recebimento de algo de valor em troca de um tratamento favorável por uma empresa, autoridade oficial ou agente público, pode ser caracterizado através de pagamentos em dinheiro e qualquer transferência de valor, tangível ou intangível.

#### **d) Administração Pública:**

Para fins da Lei, é toda a estrutura e organização do Poder Público, compreendo, União, Estados, Municípios, órgãos, empresas e pessoas (agentes públicos) que desenvolvam a atividade estatal.

#### **e) Agente Público:**

Toda pessoa que exerce, mesmo que de forma transitória ou sem remuneração, seja por eleição, nomeação, designação, contratação, concurso ou qualquer outra forma de vínculo, mandato, cargo, emprego ou função no Município, Estado, União, Órgãos Públicos ou qualquer Empresa Pública ou controlada pelos governos nacional ou estrangeiro, Fundações, Autarquias, Empresas Públicas.

### **39. POLÍTICA DE PREVENÇÃO A FRAUDES:**

No âmbito da atividade de Tecnologia é inevitável, pelas características do negócio, o convívio com a ameaça de situações de Fraude.

A fraude pode assumir diversas formas, desde as que geram a perda direta de ativos da empresa, como por exemplo o furto, a burla ou o abuso de confiança, até a adulteração de documentos, registro operacionais, sistêmicos e contábeis.

O risco de que uma situação de fraude ocorra aumenta de forma proporcional à dimensão da empresa e à complexidade inerente à sua organização e aos seus procedimentos, sistemas e produtos.

As perdas em termos financeiros podem ser consideráveis, e as consequências para a imagem devastadoras.

Tendo em conta a especificidade do conceito Fraude, a proteção total não é possível, mas podem ser tomadas medidas preventivas que tenham como objetivo reduzir o risco de ocorrência.

Neste contexto, a System Manager Tecnologia e Informática, elaborou e implementa a presente Política Antifraude, aplicável a todos quantos colaboram com a Instituição.

#### **a) Objetivo**

Esta política tem como objetivo estabelecer diretrizes claras para a prevenção, detecção e resposta a fraudes dentro da Smanager

#### **b) Âmbito**

Esta política aplica-se a todos os funcionários, diretores, fornecedores e terceiros envolvidos com a Smanager.

#### **c) Definições**

Fraude: Qualquer ato intencional de engano para obter ganho financeiro ou pessoal.

Conflito de Interesse: Situações onde interesses pessoais podem influenciar as decisões profissionais.

d) **Responsabilidades**

Funcionários: Relatar qualquer suspeita de fraude.

Gestores: Monitorar e reforçar controles internos.

Auditoria Interna: Conduzir auditorias regulares e investigar suspeitas de fraude.

e) **Medidas Preventivas**

Treinamento regular em prevenção de fraudes.

f) **Processo de Denúncia**

Relatar suspeitas de fraude através canal de denúncias

<https://smanager.com.br/canal-denuncia/>

Garantia de anonimato e proteção contra retaliação para denunciantes.

## **40. PRESENTES E ENTRETENIMENTO**

Presentes e entretenimento podem ser oferecidos e aceitos apenas como meio de mostrar boa vontade e nunca para obter vantagens comerciais inapropriadas. Não procure obter vantagens comerciais através de meios impróprios. Os presentes comerciais que comprometam ou até mesmo aparentem comprometer a habilidade de um indivíduo de tomar decisões comerciais objetivas e justas são inapropriados. Não ofereça ou aceite um presente que seja inapropriado sob as políticas da Smanager. Os parceiros comerciais que ofereçam presentes ou entretenimento considerados inapropriados podem ser desqualificados como parceiros da Smanager.

Compreende-se como “item de valor”, dinheiro, presentes, viagens, entretenimento, ofertas de emprego e refeições a trabalho. Qualquer item de valor pode também incluir patrocínio de eventos, bolsas de estudo, apoio a pesquisas e contribuições beneficentes solicitadas, ou em benefício de um agente do governo, familiares, mesmo que sejam em benefício de uma organização beneficente legítima.

Em função das penalizações impostas pela Lei, todos os colaboradores e terceiros que atuam em nome da System Manager são obrigados a cumprir as regras e procedimentos relacionados abaixo, elaborados e divulgados com o

objetivo de garantir o cumprimento das diretrizes da Lei Anticorrupção 12.846/2013.

Para garantir o cumprimento da Lei Anticorrupção 12.846/13, os colaboradores devem estar atentos para sinais de alerta que podem indicar que vantagens ou pagamentos indevidos possam estar ocorrendo.

É responsabilidade de todos os colaboradores comunicar qualquer conduta suspeita ou ação contrária às Leis 12.846/13, podendo ocorrer, também, a fiscalização de contratos, parcerias e negociações.

As comunicações de violação, identificadas ou anônimas, devem ser direcionadas ao Canal Confidencial da Companhia, um canal de comunicação independente que deve ser usado para reportar situações nas quais os valores e princípios éticos da Companhia estejam sendo colocados em risco.

Independentemente de as comunicações de violações serem identificadas ou anônimas, a System Manager tomará medidas para proteger a confidencialidade de qualquer denúncia sujeita à lei aplicável, regulamentação ou processo judicial.

Assim todo procedimento e contratos da Companhia, principalmente do governo, administração pública, devem ser obrigatoriamente passar pela análise do Jurídico e aprovado pela Diretoria Geral.

#### **41. PROFISSIONALISMO E ASSÉDIO**

Comportamentos que criem um ambiente de trabalho ofensivo não são aceitos na conduta dos negócios da Smanager, quer tenham natureza sexual ou estejam baseados em outras características do indivíduo, tais como sexo, raça, cor, origem nacional, religião ou orientação sexual.

Se você acreditar estar sendo assediado por um funcionário da Smanager, nós o encorajamos a reportar tal acontecimento à Smanager.

O assédio moral ou sexual, o abuso de poder, a intimidação, a falta de respeito e consideração, a prática de condutas lesivas à honra e integridade, a violação dos direitos fundamentais, a prática de atos atentatórios à dignidade da pessoa humana ou qualquer outro tipo de agressão física ou verbal não serão permitidos nem tolerados pela Companhia.

Isto inclui ameaças verbais ou qualquer expressão de hostilidade, intimidação, agressão.

É princípio básico de atuação na Companhia proporcionar as mesmas oportunidades no acesso ao trabalho e na promoção profissional.

A Companhia não tolera qualquer manifestação de discriminação em virtude de sexo ou orientação sexual, raça, nacionalidade, religião, origem, estado civil

ou condição social, deficiência física ou mental, bem como qualquer outro tipo de discriminação ou preconceito que possa vir a constranger a dignidade da pessoa.

#### **42. Respeito e tratamento justo**

Cumprimento de Leis e Políticas de Ação Positiva e Oportunidades Iguais de Emprego:

A System Manager oferece oportunidades iguais de emprego a todas as pessoas, independentemente de raça, religião, cor, nacionalidade, idade, sexo, deficiência física, orientação sexual ou qualquer outro fator.

Este tratamento justo aplica-se a todas as fases do vínculo empregatício, incluindo: contratação, distribuição de responsabilidades, promoção e demissão de colaboradores, oportunidades de crescimento e desenvolvimento reconhecimento de sucessos.

Os fornecedores e parceiros comerciais devem respeitar as leis trabalhistas vigentes, especialmente aquelas relacionadas a: Trabalho Infantil:

Não empregar ou não utilizar mão de obra infantil, bem como também não contratar ou manter relações com empresas que utilizem, explorem ou por qualquer meio ou forma empreguem o trabalho infantil.

#### **43. Participação em associações de classe e eventos do setor:**

Os colaboradores da System Manager podem participar de associações de classe e eventos do setor. Nessas ocasiões, é comum que se entre em contato com funcionários da concorrência.

Sempre que a participação em associações de classe e eventos do setor criar oportunidade para a legítima troca de ideias, sem a infração de leis e normas, ela será permitida e incentivada. A participação em eventos com provável presença de funcionários de concorrentes deve ser aprovada pelo presidente da unidade de negócios, pelo presidente do grupo ou pelo Conselho Executivo

#### **44. Política de Qualidade:**

A System Manager adota práticas agressivas, porém honestas de concorrência.

A System Manager fornecerá somente produtos e serviços confiáveis, que atendam plenamente as normas e regulamentações governamentais.

#### **45. PROTEÇÃO DA MARCA:**

Os fornecedores e parceiros comerciais não poderão, sem autorização prévia e por escrito da Companhia, utilizar quaisquer materiais que contenham as marcas ou produtos de propriedade da System Manager, tanto no Brasil quanto no exterior, para quaisquer finalidades, ainda que para divulgação, ficando vedada a inserção em catálogos, revistas e demais publicações, ou ainda em seu portfólio ou publicidade institucional própria.

#### **46. SAÚDE, SEGURANÇA E MEIO-AMBIENTE**

Os parceiros comerciais devem seguir as leis, regulamentos, normas e práticas aplicáveis de segurança, saúde e meio-ambiente, devendo demonstrar respeito para com seus empregados assim como para o meio-ambiente.

##### **Ações resultantes:**

A System Manager não tolerará atos de quem quer que seja, em qualquer nível da Companhia, contra pessoas que estejam cumprindo seu dever.

A System Manager não aceita que qualquer pessoa de seu quadro funcional tome qualquer tipo de atitude contra um colaborador que, de boa fé, comunique uma preocupação.

Medidas disciplinares, como, advertência por escrito, treinamentos e inclusive demissão, podem ser adotadas contra colaboradores que desobedeçam às práticas de ética empresarial da System Manager ou que, conscientemente, forneçam informações falsas.

Espera-se que os colaboradores sejam cooperativos em casos em que a empresa decida investigar alegações de má conduta ética e empresarial. Além disso, todos devem sempre ser sinceros e estar acessíveis no decorrer dessas investigações.

#### **47. PROIBIÇÃO DE DOAÇÕES ELEITORAIS:**

A Gestora não fará, em hipótese alguma, doação a candidatos ou partidos políticos via pessoa jurídica.

Em relação às doações individuais dos Prestadores de Serviço, a Empresa e seus Prestadores de Serviço têm a obrigação de seguir estritamente a legislação vigente.

## 48. Canal Direto de Conduta e Denúncias

Canal convencional de comunicação e dos recursos de ajuda disponíveis, o Canal Direto de Conduta e Denúncia é um meio simples para qualquer Colaborador reportar preocupações sobre atividades empresariais ou do local de trabalho, as quais talvez não estejam alinhadas aos Valores da System Manager. Ou para expor dúvidas, caso algum esclarecimento ou aconselhamento seja necessário. O Canal Direto de Conduta e Denúncias é um canal diretamente ligado aos responsáveis. A comunicação para esse canal pode ser feita diretamente pelo site da empresa.

Link – <https://smanager.com.br/canal-denuncia/>

[Base de Conhecimento para Consulta - Código de Ética e Compliance](#)

Ao reportar qualquer preocupação, esteja preparado para fornecer as seguintes informações sobre a situação: hora e lugar pessoas envolvidas outras informações úteis para o acompanhamento do caso.

### **Como comunicar situações preocupantes:**

Todos os colaboradores da System Manager têm o direito de fazer perguntas ou expressar preocupações sobre comportamentos no local de trabalho.

Em caso de dúvida, pergunte.

Muitas transgressões ao Código de Ética ocorrem por falta de informação ou de entendimento dos princípios, ou porque as pessoas simplesmente querem “resolver” uma situação, e não por falha de caráter ou desonestidade.

Os funcionários que, de boa-fé, buscarem aconselhamento, apontarem situações preocupantes ou reportarem comportamentos impróprios estarão cumprindo seu dever.

**Leandro Silva**  
CEO