



Estatuto de Governança e Compliance



SUMÁRIO

1. Preâmbulo	3
2. Desenvolvimento de Políticas	4
2.1. Política de Privacidade	4
2.2. Política de Segurança da Informação para Fornecedores	16
2.3. Política de Retenção e Descarte de Dados Pessoais	29
2.4. Política Anticorrupção	37
2.5. Política de prevenção e combate à lavagem de dinheiro	48
2.6. Política de responsabilidade socioambiental.....	59
2.7. Política de patrocínio, doações, hospitalidades e brindes.....	63



1. Preâmbulo

A **BALTAZAR TECNOLOGIA LTDA**, doravante denominada como (“**P4BIT**”), pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 49.452.350/0001-88, com sede na Avenida Fernanda, nº 253, Bairro Centro, Carapicuíba/SP, CEP 06.320-080.

MISSÃO: A P4BIT, como uma empresa que atua no desenvolvimento e licenciamento de programas de software customizáveis, de modo a disponibilizar às empresas públicas e privadas, especialmente, soluções de Privacidade, Segurança da Informação e Proteção de Dados, oportunizando que estas atuem em conformidade com as diretrizes previstas na LGPD, tem como missão manter os clientes plenamente satisfeitos com a qualidade dos serviços prestados, com atuação responsável, transparente, ética, auxiliando em todas as etapas do processo, como prevenção, ação, reação e conformidade, contra todo o tipo de ameaças de cibersegurança, sempre em conformidade com as normas regulatórias vigentes.

VISÃO: A P4BIT está em constante evolução e tem como visão ser reconhecida como a empresa de referência, confiável e comprometida com o oferecimento dos serviços de melhor qualidade aos seus clientes no âmbito da Privacidade, Segurança da Informação, Tecnologia e Proteção de Dados.

VALORES: Transparência e confiabilidade nas relações, respeito, responsabilidade, dedicação ao sucesso do cliente, tecnologia e constante inovação, qualidade na prestação dos serviços, segurança, proteção, e comprometimento com a ética e integridade.



2. Desenvolvimento de Políticas

A P4BIT reafirma o compromisso com a ética empresarial e a conformidade integral com as leis e regulamentos aplicáveis. Nesse sentido, disponibilizamos políticas abrangentes que delineiam as normas de conduta e os padrões éticos a serem observados por todos os colaboradores e partes envolvidas nas operações da empresa.

2.1. Política de Privacidade

2.1.1. Informações Gerais

A P4BIT compromete-se com a transparência do tratamento de dados pessoais dos nossos usuários/clientes. Privacidade e segurança são valores fundamentais e sempre adotaremos as melhores condutas para garantir a confidencialidade e integridade dos dados pessoais de clientes ou outras pessoas que se utilizam de nossas soluções e produtos. Por este motivo, elaboramos esta Política de Privacidade para esclarecer quais informações e dados pessoais serão coletados e como serão usados, compartilhados e armazenados em razão do uso dos serviços dos quais esta Política é parte integrante, sem prejuízo de outras definições atribuídas a seguir.

A P4BIT, no papel de controladora de dados, tem a responsabilidade legal de fixar a orientação dos negócios da empresa e de tratamento de dados e obriga-se ao disposto na presente Política de Privacidade.

2.1.2. Introdução

A P4BIT realiza o tratamento de dados pessoais de acordo com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Esta Política servirá como o pilar primordial para todas as práticas e processos internos promovidos pela P4BIT, relativos ao tratamento de dados pessoais que deverão ser pautados sempre de acordo com os termos aqui dispostos.

2.1.3. Conceitos básicos e definições

Alguns conceitos básicos são essenciais para melhor compreensão do usuário quanto ao tratamento de seus dados pessoais. São esses:

- **Controlador:** Controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Desta forma, a P4BIT é a responsável controladora, pertencendo a



mesma a responsabilidade das decisões sobre o tratamento dos dados pessoais fornecidos pelos Usuários e Clientes.

- **Operador:** O Operador é pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Os operadores são os colaboradores/prestadores de serviços da P4BIT que possuem acesso e autorização para realizar o tratamento de dados pessoais, os quais fazem de acordo com as diretrizes e decisões da controladora.
- **Usuário:** Pessoa física ou jurídica que acessa a plataforma e efetua cadastro mediante as condições previstas nos Termos de Uso.
- **Visitante:** Pessoa física ou jurídica que acessa a plataforma sem efetuar cadastro ou realizar pagamento.
- **Dado Pessoal:** Informação relacionada à pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível:** É o dado pessoal sobre a 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, quando vinculado a uma pessoa física natural.
- **Dado Anonimizado:** É o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Encarregado ou DPO (Data Protection Officer):** Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
- **Cookies:** Dispositivos integrados ao navegador de internet utilizados para armazenar temporariamente o que o internauta está visitando na rede.
- **Tratamento:** É toda operação realizada com dados pessoais, 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.
- **Confidencialidade:** Informação acessível ou divulgada somente às pessoas autorizadas;
- **Integridade:** Informações mantidas íntegras em seu formato original;
- **LGPD:** Lei Geral de Proteção de Dados (Lei nº 13.709/2018).

As definições trazidas pela Lei 13.709/2018, complementam as definições aqui apresentadas.



2.1.4. Princípios do tratamento de dados pessoais

A P4BIT cumprirá criteriosamente a LGPD, atuando para que os princípios abrangidos nesta Política sejam aplicados (i) no desenho e implementação de todos os procedimentos que impliquem o tratamento de dados pessoais, (ii) nos produtos e serviços oferecidos pela P4BIT, (iii) em todos os contratos e obrigações formalizadas, e (iv) na implantação dos sistemas e plataformas que permitam o acesso por parte de colaboradores ou de terceiros a dados pessoais e/ou o tratamento desses dados.

As atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios abaixo descritos. Caso alguma atividade de tratamento de dados pessoais não respeite estes princípios, ela não deve ser realizada pela P4BIT, precisando ser imediatamente revista.

- **Finalidade:** Dados pessoais somente devem ser tratados para uma finalidade específica, um propósito que seja legítimo, explícito, delimitado e informado ao titular, não sendo permitido o tratamento posterior que seja incompatível com as finalidades identificadas.
- **Adequação:** O tratamento de dados pessoais observará a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
- **Necessidade:** O tratamento de dados pessoais se limitará ao tratamento mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
- **Livre Acesso:** Será garantido aos titulares de dados, consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
- **Qualidade dos Dados:** Os dados pessoais tratados devem ser claros, exatos, relevantes e atualizados, de acordo com a sua necessidade e com os propósitos do tratamento. Não devem ser tratados dados pessoais desatualizados ou irrelevantes para a finalidade indicada.
- **Transparência:** A P4BIT prestará aos titulares de dados informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, em especial, forma e duração do tratamento, observados os segredos comercial e industrial.
- **Segurança:** A P4BIT utilizará de medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda,



alteração, comunicação ou difusão.

- **Prevenção:** A P4BIT adotará medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
- **Não Discriminação:** A P4BIT jamais realizará tratamento para fins discriminatórios, ilícitos ou abusivos.
- **Responsabilização e Prestação de Contas:** A P4BIT adotará medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, a eficácia dessas medidas.

2.1.5. As hipóteses de tratamento de dados pessoais

A P4BIT somente tratará dados pessoais de acordo com as hipóteses autorizadas pela Lei Geral de Proteção de Dados. Entre as hipóteses previstas na legislação e que são diretamente aplicáveis a P4BIT, estão as seguintes: (i) quando o titular de dados fornecer seu consentimento explícito, (ii) quando necessário para o cumprimento de obrigação legal ou regulatória, (iii) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular dos dados, (iv) quando necessário para o exercício regular de direitos em processo judicial, administrativo ou arbitral, (v) para a proteção da vida ou da incolumidade física do titular ou de terceiro, (vi) quando necessário para atender aos interesses legítimos da P4BIT ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular, e (vii) para a proteção do crédito.

2.1.6. Consentimento

Ao longo desta Política de Privacidade, informamos que alguns dados pessoais somente serão coletados pela P4BIT com o seu consentimento. Da mesma forma, esses dados somente poderão ser tratados mediante autorização e para as finalidades descritas. O consentimento é a manifestação livre, informada e inequívoca pela qual você autoriza a P4BIT a tratar seus dados.

Assim, em consonância com a Lei Geral de Proteção de Dados, seus dados só serão coletados, tratados e armazenados mediante prévio e expresso consentimento, podendo o usuário, a qualquer tempo, solicitar a sua revogação, ressalvadas as hipóteses legais previstas nesta política de privacidade.

A sua permissão será obtida de forma exclusiva para cada finalidade específica, evidenciando o compromisso de transparência e boa-fé da P4BIT para com seus usuários/clientes, seguindo as regulações legislativas pertinentes.



Ao utilizar os serviços da P4BIT e fornecer seus dados pessoais, você está ciente e consentindo com as disposições desta Política de Privacidade, garantindo, ainda, o conhecimento de seus direitos e como exercê-los.

É importante destacar que a revogação do consentimento para o tratamento dos dados pode implicar a impossibilidade da performance adequada de alguma funcionalidade do site que dependa da operação. Tais consequências serão informadas previamente.

2.1.7. Quais são os tipos de dados coletado?

A P4BIT coleta o mínimo necessário de dados pessoais para desempenhar as suas atividades. A coleta dos dados pessoais é realizada: a) durante o acesso e/ou navegação do Usuário no Website; e b) antes, durante ou após a contratação dos produtos e/ou prestação dos serviços pela P4BIT, sempre dentro dos limites da legislação aplicável. Especificamente, coletamos as seguintes informações dos Usuários e/ou Clientes, conforme o caso:

- **Dados pessoais:** A P4BIT coleta dados pessoais, que são informações que identificam o usuário ou se referem a um usuário identificável. As informações pessoais podem incluir, mas não se limitam a: nome completo, RG, CPF ou CNPJ, data de nascimento, sexo, endereço físico, endereço de e-mail, e número de telefone.
- **Dados de navegação e dispositivo:** endereço IP; o tipo de navegador do usuário e idioma; seus horários de acesso; detalhes de como o usuário usa nossos produtos e serviços; detalhes de como você gosta de interagir conosco e outras informações semelhantes.
- **Informações de pagamento:** Podemos realizar a coleta de dados bancários, tais como, identificação da instituição financeira, número da agência, número da conta de pagamento ou conta corrente, nome do titular do cartão, e Chave PIX, para fins de pagamento e/ou recebimento de valores, somente caso necessário.

Os tipos de dados e categorias especiais de dados pessoais que coletamos podem variar dependendo da espécie dos serviços fornecidos ao usuário. Em algumas circunstâncias raras, podemos também coletar outras categorias especiais de dados pessoais do usuário, seja porque você nos fornece esses dados, ou porque somos obrigados a coletá-los em decorrência de requisitos legais impostos a nós.



2.1.8. Finalidade dos dados recolhidos

Os dados recolhidos pela P4BIT serão utilizados para a prestação dos nossos serviços e terão como objetivo:

- Melhoria do serviço quanto às informações coletadas, que poderão ser utilizadas para fornecer elementos personalizados ao usuário de modo a buscar o constante aperfeiçoamento de nossos serviços;
- Personalizar o serviço para que este se adeque cada vez mais às preferências e interesses do usuário;
- Para cumprimento de obrigação legal, contratual ou legítimo interesse para retenção de dados ou necessários para fins de litígio. Neste caso, os dados serão armazenados pelo prazo de 5 (cinco) anos, contados do encerramento da obrigação;
- Para fins de registros comerciais e financeiros essenciais. Neste caso, os dados serão mantidos em nossa base de dados por até 5 (cinco) anos, após o encerramento da obrigação contratual.

2.1.9. Hipótese de compartilhamento dos dados

Os dados coletados e as atividades registradas podem ser compartilhados, sempre respeitando o envio do mínimo de informações necessárias para atingir as finalidades, conforme os casos abaixo descritos:

Destinatário	Descrição
Prestadores de Serviços	A P4BIT utiliza de prestadores de serviço, para realizar determinadas tarefas em nome da P4BIT, como processar ou armazenar dados. Os prestadores de serviço da P4BIT devem processar os dados pessoais de acordo com as diretrizes e instruções impostas.
Empresas do grupo P4BIT	A P4BIT poderá partilhar os dados pessoais com outras empresas parceiras para a realização de suas atividades diárias.
Cumprimento da Lei	A P4BIT poderá partilhar dados pessoais quando acreditar, de boa-fé, que isto é necessário para o cumprimento de uma obrigação legal nos termos da legislação aplicável, ou para responder a um processo legal válido, como, por exemplo, um mandado de busca, uma ordem judicial ou uma intimação.
Parceiros	Contamos com empresas parceiras para implementar e executar projetos e, para tanto, precisamos compartilhar os dados pessoais com eles para a efetivação da operação. Nossos



	parceiros somente são autorizados a utilizar os dados pessoais para os fins específicos que eles foram contratados, sendo obrigados ainda a tratar os dados com os padrões de segurança da informação estabelecidos por nossas políticas e bem como respeitando as cláusulas contratuais firmadas.
--	--

Caso empresas terceirizadas realizem o tratamento em nome da P4BIT de quaisquer dados pessoais que são coletados, elas respeitarão as condições aqui estipuladas e as normas de segurança da informação, obrigatoriamente.

2.1.10. Os direitos dos titulares de dados

Além da titularidade dos seus dados, os Usuários têm garantidos os direitos fundamentais de liberdade, intimidade e privacidade. Conforme o previsto na Lei Geral de Proteção de Dados (Lei nº 13.709/2018), é possível a obtenção a qualquer momento, mediante requisição, informações como: a confirmação da existência de tratamento de dados, acesso aos seus dados, correção e atualização deles, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a Lei.

Ademais, o usuário pode requerer a eliminação dos seus dados tratados, salvo em hipóteses legais contrárias e solicitar informações sobre as entidades com as quais seus dados foram compartilhados, bem como a revogação do consentimento para o uso dos seus dados.

Destacamos, ainda, os direitos do titular de dados previstos pela legislação indicada:

- I. Confirmação da existência de tratamento;
- II. Acesso aos dados;
- III. Correção de dados incompletos, inexatos ou desatualizados;
- IV. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD;
- V. Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI. Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas de cumprimento de obrigação legal ou regulatória pelo controlador e estudo por órgão de pesquisa, garantindo a



anonimização dos dados pessoais sempre que possível;

- VII. Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX. Revogação do consentimento.
- X. Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD;

Ademais, é direito do usuário receber essas informações em formato simplificado, imediatamente ou de forma detalhada, em até 15 (quinze) dias após o requerimento, conforme o disposto no art. 19 da Lei 13.709/2018.

2.1.11. Medidas de segurança dos dados pessoais

A P4BIT elenca a segurança como fator de prioridade e importância no tratamento de dados.

A P4BIT utiliza uma série de medidas físicas, eletrônicas e gerenciais para garantir que seus dados pessoais se mantenham seguros, precisos, atualizados e confidenciais, como também, armazena seus dados pessoais em ambientes operacionais que usam medidas de segurança para prevenir acessos não autorizados. Dentre as medidas utilizadas, incluem, mas não se limitam ao:

- Treinamento da equipe responsável a fim de que se encontrem cientes de nossas obrigações de privacidade e proteção de dados ao lidar com dados pessoais;
- Controle administrativo e técnico para restringir o acesso a dados pessoais.
- Medidas tecnológicas de segurança, incluindo firewalls, criptografia e software antivírus;
- Medidas de segurança física, tais como senhas e passes de segurança aos empregados para acessar nossas instalações.

Visando a devida proteção e tratamento de seus dados pessoais em conformidade com a LGPD, além das demais leis aplicáveis, a P4BIT se compromete a:

- Adotar medidas de segurança, técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;



- Manter registro das operações de tratamento de dados pessoais realizadas, especialmente quando baseado no interesse legítimo;
- Comunicar à Autoridade Nacional de Proteção de Dados e ao titular, dentro do prazo legal, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevantes aos titulares;
- Utilizar para o tratamento de dados pessoais sistemas que sejam estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD;
- Eliminar os dados pessoais após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as finalidades previstas em lei; e
- Observar as diretrizes, normas e regulamentos editados pela Autoridade Nacional de Proteção de Dados (ANPD).

Apesar de usarmos medidas de segurança apropriadas, uma vez que recebemos seus dados pessoais, a transmissão de dados pela internet nunca é completamente segura. Portanto, a P4BIT não garante que todos os dados e informações estarão livres de acessos não autorizados, principalmente caso haja partilha indevida das credenciais necessárias para o fornecimento de nossas soluções.

Desta forma, é do cliente/usuário a responsabilidade por manter tais dados de forma segura, sendo vedada a partilha de informações de acesso que possibilitem o acesso indevido, com terceiros não autorizados. Nós nos esforçamos para proteger os seus dados pessoais, mas não podemos garantir a segurança dos dados transmitidos para nós ou por nós.

No caso do operador ou controlador causarem danos ao usuário por vazamento, destruição ou corrupção desses dados, eles serão obrigados a reparar o usuário por meio de indenização nos termos da legislação brasileira, da mesma forma que não serão responsabilizados por danos nos casos presentes nessa mesma legislação.

2.1.12. Quem poderá acessar seus Dados Pessoais?

As informações pessoais coletadas somente poderão ser acessadas pelos funcionários ou agentes devidamente autorizados pela P4BIT, observando as finalidades específicas para as quais os dados pessoais tenham sido coletados.

Eventualmente, caso a inserção das suas informações aconteça em ações criadas em parcerias, os parceiros explicitamente identificados também terão acesso à informação. Nenhum dado pessoal poderá ser divulgado publicamente.



2.1.13. Por quanto tempo armazenamos os seus dados pessoais?

As informações pessoais dos usuários/clientes serão mantidas pelo tempo que for necessário para cumprir as finalidades estabelecidas nesta política de privacidade. Quanto aos dados pessoais coletados em razão da relação contratual entre as partes, poderão estes serem retidos por mais tempo para cumprimento das obrigações legais, nos termos da LGPD.

Os dados pessoais coletados são armazenados em ambiente seguro e controlado por um prazo mínimo que segue a tabela abaixo:

Período de Armazenamento	Fundamentação Legal
Enquanto durar a relação contratual e não houver pedido de exclusão ou revogação de consentimento pelo cliente/usuário.	Art. 9º, inciso II, da Lei Geral de Proteção de Dados Pessoais.
6 meses para os Dados de Identificação Digital	Art. 15 da Lei do Marco Civil da Internet.

Prazos de armazenamento superiores: Para fins de auditoria, segurança, controle de fraudes, e preservação de direitos, a P4BIT poderá permanecer com o histórico de registro de seus dados por prazo maior nas hipóteses que a lei ou norma regulatória assim estabelecer ou para preservação de direitos.

2.1.14. Cookies ou dados de navegação

A P4BIT faz uso de Cookies, que são pequenos arquivos de texto ou fragmentos enviados pela plataforma ao seu computador, smartphone ou qualquer outro dispositivo com acesso à internet e que nele se armazenam, e contêm informações relacionadas à navegação do site.

A utilização de Cookies é algo comum em qualquer plataforma digital, portanto os cookies são coletados pela P4BIT para aprimorar a sua experiência, tanto em termos de performance, como em termos de usabilidade, uma vez que os conteúdos disponibilizados serão direcionados às necessidades do usuário.

Ao acessar nosso site e consentir com o uso de Cookies, você manifesta conhecer e aceitar a utilização de um sistema de coleta de dados de navegação com o uso de Cookies em seu dispositivo.

A P4BIT recomenda que você conheça as nossas práticas como um todo, desse modo, aqui estão alguns pontos importantes para que você entenda para quais finalidades utilizamos os cookies e tecnologias semelhantes:

- Garantir o desempenho do nosso site;



- Saber quantas pessoas visitam nosso site;
- Saber quais páginas são mais populares;
- Medir o desempenho dos nossos anúncios;
- Fornecer conteúdos direcionados;
- Entender como são utilizadas nossas aplicações e ajustar o conteúdo para torná-lo mais relevante para você;
- Fornecer uma experiência melhor, mais intuitiva e satisfatória ao cliente.

Os Cookies participam deste processo, porquanto armazenam, leem e executam os dados necessários para cumprir com o nosso objetivo.

2.1.15. Categorias de cookies utilizados pela P4BIT

Os cookies que usamos geralmente se enquadram em uma das seguintes categorias:

- **Cookies Necessários:** São fundamentais para as funções básicas de navegação do nosso site. Sem eles, o site ou algumas de suas funcionalidades não operaram corretamente, prejudicando a navegação.
- **Cookies Analíticos:** Estes cookies nos permitem contar visitas e fontes de tráfego para que possamos medir e melhorar o desempenho de nosso site. Eles nos ajudam a saber quais páginas são as mais e menos populares e ver como os visitantes se movimentam pelo site. Todas essas informações que esses cookies coletam são agregadas e, portanto, anônimas.

Utilizamos cookies analíticos para definir um ID único para a sessão; coletar dados sobre o número de vezes que um usuário visitou o site, bem como datas da primeira e mais recente visita; para contar quantas vezes o nosso site foi visitado por diferentes visitantes; para identificar se um visitante é novo em nosso site, ou se já o visitou antes; para entender o comportamento em nosso site, como, por exemplo, quais páginas foram visitadas e a média de tempo gasto em cada página; dentre outras finalidades.

- **Cookies proprietários:** São cookies definidos pela P4BIT ou por terceiros em nosso nome.
- **Cookies de terceiros:** São cookies definidos por terceiros confiáveis em nossa aplicação.
- **Cookies de sessão ou temporários:** São cookies que expiram assim que você fecha o seu navegador, encerrando a sessão.
- **Cookies persistentes ou permanentes:** São cookies que permanecem no seu dispositivo durante um período determinado ou até que você os exclua.
- **Cookies de desempenho:** São cookies que otimizam a forma que nossas aplicações funcionam, coletando informações anônimas sobre as páginas acessadas.



- **Cookies de funcionalidade:** São cookies que memorizam suas preferências e escolhas (como seu nome de usuário).
- **Cookies de publicidade:** São cookies que direcionam anúncios em função dos seus interesses e limitam a quantidade de vezes que o anúncio aparece.

2.1.16. Controle de exclusão de cookies

O usuário pode, a qualquer tempo e sem nenhum custo, alterar as permissões e configurações para bloquear o uso de Cookies, recusá-los ou ser alertado quando um Cookie estiver sendo enviado para seu dispositivo, sendo necessário para isso, a consulta pelo usuário, das instruções de seu navegador. Caso você utilize dispositivos diferentes para acessar a plataforma, deverá assegurar-se de que o navegador de cada dispositivo está ajustado para atender suas preferências quanto aos Cookies.

Informamos que a desabilitação dos Cookies utilizados pela P4BIT, assim como a revogação do consentimento de determinados Cookies, pode inviabilizar o funcionamento correto de alguns recursos da plataforma, impactando diretamente na experiência do usuário. Por exemplo, talvez você não consiga visitar certas áreas de inseridas em nosso Website ou talvez não receba informações personalizadas deste.

Para gerenciar os cookies do seu navegador, basta fazê-lo diretamente nas configurações do navegador, na área de gestão de Cookies.

2.1.17. Alterações na Política de Privacidade

A P4BIT está sempre melhorando a privacidade e o tratamento de proteção de dados pessoais. Desta forma, esta Política de Privacidade pode ser atualizada a qualquer momento com efeito imediato.

A comunicação para que o cliente se certifique e consinta com as nossas atualizações será realizada através de publicação de aviso em nosso site ou por comunicado expresso via e-mail.

Ao continuar a utilizar o nosso site após a publicação das atualizações, o usuário estará a concordar com essas revisões e comprometer-se a respeitá-las integralmente.

2.1.18. Fale Conosco

Segundo a Lei nº 13.709/2018, a P4BIT é considerada a “Controladora” dos seus dados pessoais. Se após a leitura desta Política de Privacidade você ainda tiver qualquer dúvida, ou por qualquer razão precisar se comunicar conosco para realizar



solicitações envolvendo os seus dados pessoais, você pode entrar em contato pelos canais abaixo:

- **Telefone: 0800 0800 880**
- **Encarregado (DPO): contato@p4bit.com.**

Os demais pontos não abordados neste documento seguem o padrão da Lei Geral de Proteção de Dados (Lei 13.709/2018). Estamos sempre à disposição para esclarecer suas dúvidas e colocar você no controle dos seus dados pessoais.

2.2. Política de Segurança da Informação para Fornecedores

2.2.1. Introdução

A Lei Geral de Proteção de Dados (“LGPD”) exige que os controladores possuam uma Política de Segurança da Informação para Fornecedores, para gerir operações que resultem em um alto risco aos direitos e liberdades das pessoas físicas, titulares dos dados pessoais.

A Política de Segurança da Informação para Fornecedores desenvolvida pela P4BIT, foi projetada para guiar as etapas necessárias para garantir a segurança e proteção de dados da empresa e seus parceiros.

A P4BIT estabelece processos e controle para prevenção, detecção e respostas a incidentes e proteção dos dados de acessos e usos não autorizados, garantindo a gestão do risco de segurança, inclusive cibernética, como também, a construção de um alicerce robusto de segurança.

Cuidamos e restringimos o acesso aos dados na medida necessária, seguindo padrões rígidos e critérios de segurança e confidencialidade, para fornecer aos nossos colaboradores e clientes um ambiente seguro e confiável.

Usamos ferramentas e tecnologias para manter a integridade e confidencialidade das informações e protegê-las de acessos não autorizados.

2.2.2. Objetivo

Este documento tem por objetivo estabelecer padrões, normas e diretrizes a serem seguidas por fornecedores e colaboradores para o correto acesso e manuseio de informações de forma a assegurar a confidencialidade, integridade e disponibilidade destas em seu ambiente físico e virtual.



2.2.3. Aplicação

Esta política aplica-se aos fornecedores e prestadores de serviço que têm acesso e autorização para alterar a confidencialidade, integridade e disponibilidade de informações repassadas pela P4BIT.

2.2.4. Referências

- ABNT NBR ISO/IEC 27001:2022;
- ABNT NBR ISO/IEC 27002:2022;
- Lei Geral de Proteção de Dados (LGPD) 13.709/18;

2.2.5. Conceitos básico e definições

- **Colaborador:** Diretores, funcionários, estagiários, terceiros e prestadores de serviços.
- **Dispositivos Móveis:** Notebooks, tablets, smartphones, celulares, modems 3/4G.
- **Fornecedor:** É toda pessoa física ou jurídica que desenvolve atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
- **Incidentes de Segurança da Informação:** Eventos de segurança da informação relacionados e identificados, que podem prejudicar ativos da organização ou comprometer sua operação.
- **Mídias Removíveis:** Refere-se ao tipo de memória que pode ser removida do dispositivo, conferindo portabilidade para as informações ali inseridas, alguns exemplos são: CD's/DVD's, pen drive, HD externo, leitores de cartão de memória etc.
- **Segurança da Informação:** Competência que visa proteger a informação contra ameaças e vulnerabilidades buscando garantir a continuidade do negócio e minimização de riscos, alinhado com os objetivos estratégicos de negócio. Adicionalmente, zela pelos princípios de confidencialidade, integridade, disponibilidade e autenticidade.
- **Usuários:** Colaboradores e terceiros que tenham acesso a qualquer Informação em decorrência de suas atividades e prestação de serviços para a P4BIT, seja em ambiente próprio ou terceirizado, localizado dentro ou fora das instalações da P4BIT.
- **Visitante:** Todo indivíduo que não possui vínculo trabalhista ou contrato de prestação de serviço.



- **Wireless:** Infraestrutura de comunicação sem fio para transmissão de dados e informações, também conhecida como Wi-Fi.

2.2.6. Descrição Geral

2.2.6.1. Introdução ao SGSI

O Sistema de Gestão de Segurança da Informação (“SGSI”) da P4BIT tem por objetivo garantir a adoção de medidas alinhadas com as estratégias de negócio, realizando o monitoramento dos processos e ações, buscando a melhoria contínua e a proteção do ambiente. A P4BIT estabeleceu seu sistema de gestão voltado para Segurança da Informação, que define diretrizes para estabelecer, implementar, manter, monitorar e gerenciar um Sistema de Gestão Segurança da Informação.

O objetivo da área de segurança da informação é preservar a confidencialidade, integridade e disponibilidade da informação, por meio da manutenção e melhoria contínua do Sistema de Gestão da Segurança da Informação e dos controles de segurança adequados para proteção dos ativos da P4BIT.

2.2.6.2. Responsabilidades

- **Área de Segurança da Informação**
 - Identificar os requisitos de segurança da informação aplicados pelo fornecedor durante toda a cadeia de suprimentos;
 - Definir o processo de avaliação de fornecedores de forma a mitigar os riscos e validar as aplicações e/ou serviços de TI;
 - Realizar a análise crítica dos requisitos de segurança dos novos contratos de fornecedores de TI e/ou a cada renovação;
 - Realizar a revogação de todos os direitos de acesso às informações após o encerramento dos serviços/atividades prestadas pelos fornecedores e parceiros mediante notificação do Gestor do Contrato;
 - Realizar a revogação de todos os direitos de acesso às informações para os casos de descumprimento de diretrizes da Política de Segurança da Informação para Fornecedores.
 - Reportar ao time de Riscos e Controles internos os fornecedores de risco elevado conforme diligência realizada.
- **Área de Compras e Contratos**
 - Zelar para que os fornecedores tenham acesso e ciência da Política de Segurança da Informação para Fornecedores e o registro do comprometimento em atender os requisitos de segurança da informação definidos nesta política.



- Controlar o checklist da documentação apresentada pelos fornecedores através do sistema interno para monitoramento do workflow de aprovação.
- **Fornecedores**
 - Manter-se atualizado sobre a Política de Segurança da Informação para Fornecedores da P4BIT;
 - Comprometer-se em manter a segurança e atender aos requisitos definidos nesta Política;
 - Realizar a divulgação aos profissionais que realizarão atividades com a P4BIT e assegurar que assinem o registro “Aceitação da Política de Segurança da Informação”.

2.2.6.3. Critérios e Diretrizes

- **Aspectos Gerais**

Para que os objetivos de Segurança da Informação sejam alcançados, as seguintes diretrizes devem ser seguidas e consideradas em todas as atividades realizadas dentro ou fora das dependências da P4BIT, sempre que exista a necessidade de manipulação de suas informações:

- Todas as atividades inerentes à Segurança da Informação devem estar em conformidade com esta Política de Segurança da Informação para Fornecedor da P4BIT; e
- Todos os recursos e informações devem ser protegidos nos quesitos: confidencialidade, integridade e disponibilidade;
- Todos os fornecedores que prestam serviços em nuvem devem assegurar salvaguardas para o gerenciamento, aquisição e suporte à segurança da informação;
- Todo o acesso deve ser único e manter trilhas de auditoria contendo, no mínimo, endereço IP de origem da chamada, porta de comunicação origem da chamada (porta TCP do cliente), data, hora, sistema, usuário (quando aplicável), objeto, falha ou sucesso da ação das configurações realizadas nos sistemas e meios relacionados a prestação de serviço, observadas a legislação e regulamentações vigentes.
- Todos os fornecedores se comprometem a manter seus colaboradores conscientizados periodicamente de acordo com os procedimentos de segurança da informação, bem como orientados devidamente de seus papéis e responsabilidades;
- Todos os fornecedores envolvidos nas atividades da P4BIT, devem estar cientes da presente Política de Segurança da Informação para Fornecedores, assim como possuir suas próprias políticas de segurança da



informação, controle de acesso lógico, dispositivos móveis, mídias removíveis, continuidade da segurança da informação, gestão de mudanças, gestão de incidentes, mesa e tela limpas e outras;

- Todo contrato com fornecedor ou prestador de serviço que envolva: Serviços de tecnologia, Manipulação de dados ou Tecnologia, deve conter o Anexo Requisitos de Segurança da Informação para Fornecedores e Prestadores de Serviços;
- Todos os equipamentos que processam informações pertencentes à P4BIT, devem possuir solução antivírus atualizada, controles de acesso remoto, incluindo, mas não se limitando a autenticação de dois fatores acesso ao dispositivo por VPN (Virtual Private Networking) e portas de protocolos restritos; , :
- Todos os fornecedores se comprometem a manter um inventário atualizado dos ativos de hardware e softwares;
- Todos os fornecedores se comprometem a não permitir a utilização de equipamentos pessoais ou não monitorados para a prestação de serviços;
- Todos os fornecedores se comprometem a notificar e informar P4BIT sobre a subcontratação de serviços relevantes no prazo máximo de 5 (cinco) dias úteis. à ,
- Quando solicitado, o fornecedor se compromete a responder, no prazo máximo de 15 (quinze) dias úteis, a avaliação de diligências de segurança da informação.
- Não é permitido a realização de testes de invasão, brute force ou qualquer ação que esteja caracterizada como acesso indevido.
- **Propriedade da Informação**
 - Toda informação gerada dentro ou fora da P4BIT a respeito de seus dados é de seu domínio, não importando a data de criação ou forma de representação e transporte. O sigilo das informações criadas ou acessadas deve ser mantido mesmo após encerramento das atividades no ambiente.
 - O cumprimento desta Política de Segurança da Informação e a preservação do sigilo das informações e de dados sensíveis da empresa é um dever de todos. É vedada a reprodução de quaisquer documentos, dados ou informações da P4BIT, sem o expreso consentimento desta, através de autorização de representante com poderes para tanto.
- **Classificação da Informação**
 - As informações de propriedade da P4BIT devem ser utilizadas exclusivamente com propósitos de negócios e o acesso a elas dependerá da função exercida e da autorização prévia do responsável pela informação.



Todas as informações estão classificadas no documento Classificação de Sigilo das Informações, de acordo com a sua sensibilidade para o negócio, conforme os critérios estabelecidos neste documento sendo utilizados os seguintes rótulos:

- Altamente confidencial
 - Confidencial
 - Interno
 - Geral
- Todos os documentos pertencentes P4BIT, possuem um rótulo de classificação. O manuseio de qualquer informação independente de sua classificação deve ocorrer com o mínimo de exposição, no que se refere ao armazenamento/transmissão (uso de criptografia, cofres ou armários com chaves) e descarte. à Informações Altamente Confidenciais
 - Considera-se como Alto Nível de Segurança, as informações extremamente sensíveis, que se divulgadas indiscriminadamente ocasionam sérios prejuízos ou consequências no âmbito de negócio, financeiro, legal e/ou estratégico para P4BIT, seus clientes e colaboradores. Exemplos: dados pessoais sensíveis como origem racial ou étnica, posicionamento político, crenças religiosas, crenças filosóficas, filiação sindical, dados genéticos, dados biométricos, dados de saúde, vida sexual e orientação sexual. À
 - O acesso a estas informações é restrito a um grupo específico de pessoas e deve ser controlado. A divulgação de informações com esta classificação só é permitida mediante autorização prévia do proprietário da informação.
- **Informações Confidenciais**
 - Considera-se como confidencial, as informações que se divulgadas, podem causar impactos adversos para a empresa, clientes, fornecedores e/ou colaboradores. Exemplos: informações estratégicas da companhia, dados pessoais, dados financeiros, dados de negócio, informações relacionadas aos órgãos estatutários ou não estatutários da companhia, licitações e contratos.
 - O acesso a estas informações é limitado a um grupo específico de pessoas e deve ser controlado. A divulgação de informações com esta classificação só é permitida mediante autorização prévia do gestor ou proprietário da informação.
 - **Informações Internas**
 - Consideram-se como internas, as informações que são de uso comum dos colaboradores e atividades laborais e que podem deixar a empresa vulnerável se divulgadas externamente. São informações que devem



circular somente no ambiente interno da P4BIT. Exemplos: normativos internos, desenvolvimento de programas internos da empresa, resultados não públicos.

- **Informações Gerais**

- Consideram-se como gerais as informações públicas cuja divulgação irrestrita não causa nenhum impacto ou perda para a P4BIT. Exemplos: manual de produto, balanço patrimonial, demonstrações financeiras, informações para licitações, folders, campanha publicitária, reportagens para revistas e jornais, material de divulgação de produtos ou serviços.

- **Informações sem Rótulo**

- As informações ainda não classificadas devem ser consideradas como confidenciais. Em casos de acesso, manuseio, armazenamento, transporte ou transmissão, o colaborador ou custodiante deverá consultar o proprietário da informação ou pessoa autorizada por ele, visando obter a confirmação da classificação adequada da informação.

- **Descarte das informações**

- Os fornecedores devem comprometer-se a implementar políticas e procedimentos para garantir que a informação repassada pela P4BIT seja destruída de forma segura, quando não for mais necessária para os fins autorizados por ela. Assim, se faz necessário confirmar antes do descarte dos ativos, que as informações da P4BIT foram apagadas de forma adequada, mantendo o registro da destruição.
- Em casos que há terceiro contratado envolvido para o processamento da informação da P4BIT, deve ser garantido que o mesmo, descarte de forma segura as informações, quando estas não se fizerem mais necessárias.

- **Segurança nas Comunicações**

- Os fornecedores devem comprometer-se a segregar logicamente ou fisicamente os dados da P4BIT dos demais clientes.
- Também devem assegurar a implementação de procedimentos de filtragem dos acessos à Internet, para proteger as estações de trabalho do usuário final de sites mal-intencionados e transferências de arquivos não autorizados. As informações da P4BIT devem ser criptografadas quando em repouso.
- As atividades de compartilhamento e transmissão da informação devem ser realizadas através dos meios seguros, homologados pela Segurança da Informação da P4BIT.

- **Uso da Internet**

- Para casos em que a atuação in loco seja necessária, o uso de conexões aos



sistemas de internet é permitido para atender apenas propósitos de negócios da P4BIT, tendo a empresa o direito a qualquer momento, de:

- Suspende o acesso do fornecedor;
 - Restringir o download e upload de arquivos ou acesso a conteúdo que não sejam de interesse da empresa;
 - Monitorar e auditar os acessos;
 - Solicitar aos fornecedores justificativas por acessos efetuados.
- É expressamente vedado o uso dos recursos da P4BIT para:
 - Acesso ou veiculação de conteúdo relacionado à pedofilia;
 - Veiculação de conteúdos de cunho: político, religioso, racial, orientação sexual, pornográfico e ilegal (pirataria de software, comércio de ilícitos etc.) e quaisquer outros conteúdos que contrariem as boas práticas ou que prejudiquem a imagem e a honra da empresa;
 - Quaisquer outras atividades consideradas inapropriadas, indevidas ou desvinculadas às atividades desempenhadas na empresa;
 - Publicar, postar, carregar, distribuir, compartilhar ou divulgar quaisquer tópicos, nomes, materiais ou informações que incentivem a discriminação, ódio ou violência com relação a uma pessoa ou a um grupo;
 - Uso de falsa identidade ou assumir, sem autorização, a identidade de outro usuário;
 - Utilizar-se da internet e outros serviços disponibilizados com o intuito de cometer crime ou fraude;
 - Utilizar os serviços, para de qualquer modo reproduzir ou infringir direitos de terceiros, sejam imagens, áudio, fotografias, vídeos, softwares ou qualquer material protegido por lei de propriedade intelectual, incluindo, lei de direitos autorais, marcas ou patentes;
 - Fins ilícitos, tais como: atividades hackers, crackers, bombas, falsidade ideológica, entre outros;
 - A utilização da rede Wireless Corporativa por dispositivos não homologados pela P4BIT. Em caso de exceção para prestadores de serviço e terceiros que desenvolverão projetos de longo prazo, é necessário abrir uma solicitação ao Service Desk, devendo passar pela aprovação do gestor imediato;
 - **Backup**
 - Os fornecedores devem realizar periodicamente o procedimento de execução de backups e testes de restore nos ativos que armazenam



informações da P4BIT, a fim de evitar ou minimizar a perda de dados em caso de incidentes, quando aplicável.

- A P4BIT exige que toda mídia armazenada fora seja criptografada e as chaves de segurança armazenadas em um cofre corporativo. de sua infraestrutura

- **Tecnologia em Nuvem**

- Aos fornecedores que possuem serviços em nuvem, é recomendado salvaguardar o gerenciamento, a aquisição e o suporte à Segurança da Informação nesses serviços, de modo a garantir a confidencialidade, integridade e disponibilidade das informações presentes no sistema operacional.
- A P4BIT também orienta assegurar a criptografia dos dados em trânsito e repouso nas camadas de aplicação e de interfaces.
- É indicado definir e documentar a Política de Utilização de Serviços em Nuvem que contemple as estratégias de adesão desses serviços, visando o cumprimento da legislação e da regulamentação em vigor e descrevendo como se realizará a substituição de prestadores de serviços em nuvem no caso de descontinuidade ou necessidade.
- Sempre informar aos representantes da P4BIT o mais rápido possível sobre a contratação de fornecedores de armazenamento e processamento de dados em nuvem, indicando qual a empresa selecionada, quais os serviços e, se possível, quais os países e regiões onde os dados serão armazenados, processados e gerenciados.

- **Controle de Acesso**

- Os fornecedores devem possuir controles de acesso à informação, a fim de protegê-la contra possíveis danos, acessos não autorizados ou perdas. Para isso, devem ter uma Política de Controle de Acesso que descreva as diretrizes para a criação, alteração, revisão e exclusão de contas de usuários para sistemas ou aplicativos.
- Os privilégios da conta do usuário devem ser realizados com base no princípio do privilégio mínimo necessário e devem ser formalmente autorizados e registrados.
- Os direcionadores sobre uso de senha segura e duplo fator de autenticação devem ser formalmente registrados, contendo todas as precauções necessárias para cuidar das credenciais de acesso e protegê-las contra acesso não autorizado.
- Quando aplicável para a prestação do serviço, o Fornecedor deve credenciar nos domínios da P4BIT seus profissionais autorizados a operar



presencialmente e remotamente aqueles que terão acesso aos sistemas corporativos, inclusive com a assinatura de termo apropriado de sigilo e responsabilidade.

- O fornecedor se responsabiliza por comunicar a P4BIT, com antecedência de no mínimo 1 (um) dia útil, qualquer término ou mudança de responsabilidades de emprego de funcionários envolvidos diretamente na execução dos serviços de suporte à infraestrutura, a fim de que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da P4BIT, caso aplicável a esta contratação.

- **Gestão de Vulnerabilidades**

- O fornecedor deve implantar um programa corporativo de gestão de patches e vulnerabilidades para verificar se ativos de hardware e software possuem vulnerabilidades conhecidas e geri-las.
- Os fornecedores devem realizar testes de segurança anuais (Pentest), com empresa independente se possível, a fim de assegurar que os controles de segurança estão devidamente implementados.
- Os relatórios deverão ser compartilhados com a P4BIT sempre que esta entender necessário, ficando o fornecedor responsável por solucionar todas as vulnerabilidades.
- O Fornecedor terá os seguintes prazos, a contar da data de comunicação da vulnerabilidade à P4BIT, para providenciar o plano de correção, que deverá ser validado por esta:
 - Alta vulnerabilidade: até 07 (sete) dias corridos;
 - Média vulnerabilidade: até 14 (catorze) dias corridos;
 - Baixa vulnerabilidade: até 21 (vinte e um) dias corridos.
- A P4BIT poderá solicitar a execução dos testes de Segurança da Informação (Pentest) na infraestrutura que suporta a operação, desde que comunicado previamente com 10 (dez) dias úteis de antecedência.

- **Desenvolvimento e Manutenção de Sistemas**

- Os fornecedores devem manter controles de alteração projetados para atender aos requisitos de segurança dos sistemas de informação desenvolvidos internamente e relacionados à prestação de serviços, bem como realizar a revisão e testes de código periodicamente.
- Também devem separar logicamente ambientes para desenvolvimento, teste e produção. O acesso dos usuários aos ambientes e informações da P4BIT devem ser restritos e segregados, com base nas responsabilidades do trabalho atribuído.
- As alterações dos softwares e infraestrutura devem ser autorizadas e



formalmente documentadas, testadas, revisadas e aprovadas, antes da migração do ambiente não produtivo para o ambiente de produção.

- Os dados de produção da P4BIT não devem ser usados para realização de testes em qualquer ambiente produtivo e não produtivo.

- **Gestão de Mudanças**

- Os fornecedores devem possuir um processo de gestão de mudanças com o intuito de controlar as alterações nos sistemas de produção, rede de produção, aplicativos, arquivos de dados estruturais, outros componentes do sistema e mudanças físicas/ambientais, através de um registro formal de controle de mudança, minimizando os impactos e riscos associados à manutenção do serviço.

- **Resposta a Incidentes de Segurança da Informação**

- Os fornecedores devem ter um plano de resposta a incidentes de segurança da informação que inclua qualquer evento de Segurança da Informação que perturbe ou que possa interromper um serviço. O plano deve detalhar os processos de tratamento de incidentes para detectar, triar, responder e gerir o pós-incidente que afete as redes e/ou sistemas.
- Além disto, o fornecedor informará P4BIT, em no máximo 24 (vinte e quatro) horas após o conhecimento do incidente de segurança, a respeito de qualquer natureza envolvendo informações da P4BIT, através do endereço de e-mail: contato@p4bit.com, as seguintes informações:
 - Data e hora do incidente;
 - Data e hora da ciência do incidente;
 - Qual o tipo de incidente de segurança;
 - Descrição do incidente;
 - Indicação de medidas adotadas para contenção e prevenção dos riscos associados.
- Caso ocorra mais de um Incidente de Segurança no período de 90 (noventa) dias corridos, poderá ser exigido que o fornecedor, às suas expensas, contrate uma empresa de segurança para avaliar as suas medidas protetivas. A contratada deverá ser previamente aprovada pela P4BIT.
- O fornecedor deverá compartilhar o relatório de avaliação com a P4BIT e compromete-se a corrigir todas as vulnerabilidades identificadas durante a avaliação.
- Se o fornecedor, seus colaboradores ou terceiros forem responsáveis por um incidente de segurança, independentemente de este ocorrer por descumprimento do contrato ou falha em notificar a P4BIT, este compromete-se a realizar o reembolso por todos os danos e custos devidos



em razão dos atos e/ou omissões, ficando responsável pelo pagamento das despesas incorridas na investigação e remediação do incidente de segurança.

- **Continuidade da Segurança da Informação**
 - O fornecedor deve comprometer-se a manter a continuidade das operações de Segurança da Informação, com o objetivo de minimizar as perdas e manter a operacionalidade dos sistemas em situações adversas, como, por exemplo, situações de crise ou desastre.
- **Auditorias e Análise de Riscos**
 - Os fornecedores devem permitir que a P4BIT monitore e avalie os serviços contratados por meio de diligências, desde que avisada previamente com mínimo de 10 (dez) dias úteis, a aderência aos requisitos contratuais, incluindo os controles de Segurança da Informação. Sendo assim, comprometem-se a disponibilizar sua documentação, relatórios e/ ou informação comprobatória durante a diligência.
 - Os fornecedores devidamente certificados pela ISO 27001 não precisarão realizar esse processo de auditorias e análise de riscos, desde que apresentem a comprovação da vigência da certificação para o escopo contratado e ele seja validado pela área de Segurança da Informação da P4BIT.

2.2.7. Aceitação da Política de SI para Fornecedores

Ao iniciar as atividades de prestação de serviço que envolvam informações da P4BIT, os fornecedores deverão ter acesso à “Política de Segurança da Informação para Fornecedores”, e realizar o aceite desta, visando documentar o seu comprometimento em manter a segurança e atender aos requisitos definidos, realizando a divulgação a todos os envolvidos nas atividades relacionadas à prestação de serviços à P4BIT.

2.2.8. Segurança no Relacionamento com Fornecedor

Os fornecedores devem assegurar que seus subcontratados e prestadores de serviços que possuem acesso às informações da P4BIT tenham, no mínimo, os mesmos controles e procedimentos de Segurança da Informação descritos nesta Política.

Os acordos com essas partes devem ser revisados periodicamente para assegurar que a segurança da informação e os requisitos de proteção de dados permaneçam apropriados.



2.2.9. Descumprimento da Política de Fornecedores

Caso seja identificado o descumprimento referente a esta Política, a P4BIT poderá revogar os acessos e avaliar as violações para definir as ações necessárias, conforme estabelecido no contrato de prestação de serviço firmado entre a P4BIT e o Fornecedor. , sem prejuízo das demais sanções cabíveis nos termos da legislação brasileira. Esta política não anula e não substitui o contrato estabelecido entre as partes.

2.2.10. Continuidade do Negócio e Plano de Recuperação

O Fornecedor estabelecerá e manterá planos de contingência, recuperação e controles apropriados de riscos para garantir a execução continuada segundo o Contrato Master. Os planos deverão estar estabelecidos em 30 (trinta) dias após a data efetiva deste Anexo e deverão incluir, mas não se limitar a testes, funções de controle, responsabilidade e ações corretivas a serem implementadas imediatamente, caso necessário. O Fornecedor concorda em permitir o acesso da P4BIT aos planos em um horário mutuamente convencionado.

2.2.11. Do Cumprimento às Leis Anticorrupção

O Fornecedor garante e declara não ter conhecimento de que seus fornecedores, empregados, prepostos ou qualquer pessoa a quem o Fornecedor subcontrata para prestação de qualquer parte do contrato firmado com a P4BIT, tenham sido condenados ou sejam sujeitos de qualquer inquérito, investigação ou processo criminal promovidos por qualquer instância ou órgão público, órgão administrativo ou regulador em relação a qualquer crime ou alegação de crime em relação às leis anticorrupção.

O Fornecedor obriga-se a notificar a P4BIT assim que tomar conhecimento de que qualquer dos seus fornecedores, funcionários, prepostos ou pessoas associadas tenham se comportado de forma que enseje possível violação às Leis Anticorrupção.

O Fornecedor solicitará que cada pessoa associada expressamente concorde com as obrigações contidas nesta cláusula e nas Leis Anticorrupção.

O Fornecedor concorda em (i) manter políticas e procedimentos anticorrupção adequados para garantir que todos seus fornecedores, empregados, prepostos e pessoas associadas possam cumprir as Leis Anticorrupção (ii) fornecer uma cópia de suas políticas e procedimentos anticorrupção à P4BIT quando solicitado e (iii) fiscalizar e impor suas políticas e procedimentos anticorrupção.



"Pessoa Associada" significa qualquer pessoa a quem Fornecedor subcontrata para a prestação de qualquer elemento do contrato com a P4BIT, ou que recebe quaisquer serviços relacionados com o cumprimento do contrato pelo Fornecedor.

2.3. Política de Retenção e Descarte de Dados Pessoais

2.3.1. Introdução

A P4BIT tem a responsabilidade de garantir a adequação com Lei Geral de Proteção de Dados ("LGPD") que exige que os controladores possuam uma Política de Retenção e Descarte de Dados Pessoais para atender às determinações relativas ao tratamento de dados.

A Política de Retenção e Descarte de Dados Pessoais desenvolvida pela P4BIT foi projetada para guiar as etapas necessárias ao atendimento da LGPD, respeitando os direitos dos Titulares e conferindo transparência e segurança ao processo da P4BIT.

Através da presente Política, realizamos o descritivo de todas as etapas que compõem o armazenamento das informações e requisitos de descarte.

A P4BIT estabelece processos e controles para prevenção, detecção e respostas a incidentes e proteção dos dados contra acessos e usos não autorizados, garantindo a gestão do risco de segurança, inclusive cibernética, e a construção de um alicerce robusto de segurança.

Cuidamos dos dados, seguindo padrões rígidos de segurança e confidencialidade, para fornecer aos nossos colaboradores um ambiente seguro e confiável. Usamos ferramentas e tecnologias para manter a integridade e confidencialidade das informações e protegê-las de acessos não autorizados.

Adicionalmente, restringimos os acessos aos dados na medida necessária, com rígidas obrigações de confidencialidade e sigilo e mediante a adoção de critérios de segurança. As diretrizes de proteção dos dados da organização, dos colaboradores, dos clientes e do público geral estão formalizadas na Política de Segurança da Informação, Política de Privacidade, e Diretiva de Proteção de Dados dos Colaboradores.

2.3.2. Retenção e descarte de Dados Pessoais

A P4BIT tem a responsabilidade de garantir o cumprimento à Lei Geral de Proteção de Dados (LGPD) e seus requisitos relativos à coleta, armazenamento, recuperação e destruição de registros de dados pessoais e/ou dados sensíveis ("Dados Pessoais").



Esta política complementa, mas não substitui, a Política de Privacidade de Dados da P4BIT, e outras políticas afins existentes.

A P4BIT mantém conjuntos de Dados Pessoais armazenados (“Registros”) em conformidade com requisitos contratuais, regulatórios e demais bases legais aplicáveis às modalidades de tratamentos de Dados Pessoais. É importante que esses Registros sejam protegidos contra perda, destruição, falsificação, acesso não-autorizado e liberação não-autorizada. Para isso, uma variedade de controles é utilizada, como backups, controle de acesso e criptografia.

Esses controles se aplicam a todas as operações, pessoas e processos que constituem o sistema de informações da P4BIT, incluindo colaboradores, membros do conselho, diretores, fornecedores, clientes e terceiros que têm acesso aos dados tratados pela P4BIT.

2.3.3. Programa Geral de Retenção

A Equipe de Proteção de Dados da P4BIT define o período durante o qual os documentos e registros devem ser retidos por meio do Calendário de Retenção de Dados.

Poderão existir exceções aos períodos de retenção no Calendário de Retenção de Dados, nos seguintes casos:

- Investigações em andamento das autoridades, caso haja a necessidade de registros de dados pessoais por parte da empresa, para comprovar o cumprimento de quaisquer requisitos legais; ou
- Para exercício dos direitos legais em casos de processos judiciais com base na legislação vigente.

2.3.4. Classificação de Registros

A P4BIT classifica os Registros em categorias que estabelecem os requisitos de retenção e de descarte para cada uma das espécies. Todos os dados pessoais são retidos pelo tempo necessário ao cumprimento do objetivo para os quais foram coletados, com finalidades lícitas, específicas e informadas.

Há uma diversidade de tratamentos de dados pessoais cujo prazo de arquivamento não é determinado por lei, como por exemplo, o tempo de guarda dos dados pessoais de um prospect comercial. Para tais dados, a P4BIT estipula um prazo de guarda que seja coerente com as práticas de mercado e com a natureza do tratamento, enquanto não houver determinação específica pela autoridade reguladora.



Para os demais registros, incluindo aqueles de ordem tributária, trabalhista e previdenciária, a P4BIT se reserva o direito de mantê-los armazenados até o fim do prazo prescricional estipulado em lei.

2.3.5. Categorias de Registros

- **Registros de Negócios:** informações registradas em qualquer meio, criadas ou capturadas que reflitam circunstâncias, eventos, atividades, transações ou resultados criados ou mantidos como parte da condução de negócios da P4BIT, como por exemplo, venda de produtos do portfólio; celebração e execução de contratos; e análise e proteção do crédito.
- **Registros de Marketing e Comunicação:** informações pessoais obtidas pela P4BIT em: (i) campanhas publicitárias; (ii) ações promocionais e pesquisas; (iii) redes sociais; e (iv) serviço de atendimento ao consumidor - SAC. Os registros que forem utilizados para fins de marketing ou de pesquisa permanecerão armazenados na base da P4BIT, apenas enquanto perdurar o interesse do titular em receber esses materiais, sendo possibilitado o opt-out a qualquer tempo, o qual permite a revogação do consentimento, caso esta seja a base legal que fundamente a respectiva modalidade de tratamento.
- **Registros de Segurança:** informações coletadas para gerenciamento do acesso e permanência nas instalações da P4BIT como nome, RG, CPF, foto, biometria, controle de crachá, instalações por CFTV, login e senha para acesso aos sistemas de informação.
- **Registros de Recursos Humanos:** dados pessoais coletados para (i) gestão do RH, como por exemplo, gerenciamento de tempo de trabalho, salários, benefícios, contribuições previdenciárias e impostos; férias, licenças e ausências; (ii) gestão de carreira, como treinamentos, avaliações, experiência profissional e mobilidade da P4BIT (iii) administração do RH para comunicação corporativa, trabalho em rede social da empresa e uso de ferramentas de computador e telefonia; organogramas, serviços corporativos, planejamento e orçamentos, relatórios, pesquisa, reorganizações, aquisições e cisões; (iv) saúde ocupacional, como atestados médicos, prontuário médico, atestados de saúde ocupacional e todos os demais relacionados à saúde do colaborador; (v) recrutamento e seleção, como nome, gênero, estado civil, idade, dados de contato, RG, CPF, CNPJ, comprovante de endereço, dados bancários, informações de função, habilidades, experiências, qualificações, referências, currículo, dados de entrevista e avaliação, notas e registros da entrevista e qualquer outra informação que o candidato disponibilize para a P4BIT; e (vi) gestão de viagens de negócios, como informações para organização de viagens



(preferências, local etc.); CNH e despesas.

Alguns dados pessoais são retidos após o término do contrato de trabalho, estágio ou contrato de prestação de serviços para cumprir os períodos legais de armazenamento definidos pela legislação trabalhista, tributária, e de proteção de dados.

Os contratos de trabalho, as fichas de registro de colaboradores e os respectivos Perfis Profissiográficos Previdenciários (PPP) serão armazenados por período indeterminado, mesmo após a rescisão contratual.

Tipo de Registro	Descrição	Período de Retenção	Formato de Descarte
Negócios	Contato Comercial (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail)	01 ano após contato inicial sem resposta, ou prontamente, no caso de revogação do consentimento ou da manifestação de desinteresse em ser contatado	Eliminação pela P4BIT, opt-out, ou a qualquer tempo pelo titular
Negócios	Documentos Tributários	5 anos a contar da data de emissão do documento	Eliminação pela P4BIT
Negócios	Proteção do Crédito (nome; cargo; RG, CPF, endereço; país de origem, profissão, telefone; e-mail)	Durante relação comercial e mais 5 anos após o término ou prontamente, em caso de exaurimento da finalidade	Eliminação pela P4BIT
Marketing e Comunicação	Campanhas Publicitárias, Ações Promocionais e Pesquisas (nome, RG, CPF, endereço, país de origem, e-mail, telefone,	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou revogação do consentimento	Eliminação pela P4BIT ou Opt-out a qualquer tempo pelo titular



	respostas a pesquisas)		
Marketing e Comunicação	Site e Redes Sociais (dados de geolocalização, endereço de IP, dados on-line capturados, cookies)	12 meses após a última atividade ou prontamente após revogação do consentimento	Eliminação pela P4BIT ou Opt-out a qualquer tempo pelo titular
Marketing e Comunicação	Serviço de Atendimento ao Consumidor – SAC (nome, telefone, e-mail, endereço e CPF)	5 anos após o último atendimento	Eliminação pela P4BIT
Recursos Humanos	Gestão de RH	Durante Contrato de Trabalho e mais 5 anos após o término, exceto FGTS (30 anos) e Folha de Pagamento (10 anos) Armazenamento de Contrato de Trabalho: prazo indeterminado	Eliminação pela P4BIT
Recursos Humanos	Gestão de Carreira	Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pela P4BIT
Recursos Humanos	Administração do RH	Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pela P4BIT

2.3.6. Retenção de Descarte de Dados

Para cada um desses cenários, a tabela a seguir mostra o período máximo de retenção de dados pessoais pela P4BIT, por categoria de registro, descrição, bem como o formato de descarte:



Recursos Humanos	Saúde Ocupacional	Durante o contrato de trabalho e mais 20 anos após a rescisão contratual	Eliminação pela P4BIT
Recursos Humanos	Recrutamento e Seleção	Indeterminado ou prontamente, em caso de exaurimento da finalidade ou após revogação do consentimento Aprovação do candidato: Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pela P4BIT ou Opt-out a qualquer tempo pelo titular
Recursos Humanos	Gestão de Viagens de Negócios	Durante Contrato de Trabalho e mais 5 anos após o término	Eliminação pela P4BIT
Segurança	Acesso às instalações físicas da P4BIT (dados biométricos, nome, foto, RG, CPF)	5 anos após o último acesso	Eliminação pela P4BIT
Segurança	Sistema CFTV (imagens)	Eliminação pela P4BIT	Eliminação pela P4BIT
Segurança	Acesso ao sistema de informação da P4BIT (login e senha)	5 anos após o último acesso	Eliminação pela P4BIT
Dados de Clientes	Dados fornecidos por Clientes	De acordo com o SLA definido pelo Cliente	Eliminação pela P4BIT



2.3.7. Eliminação pela P4BIT

Assim que o período determinado expirar, e desde que não haja uma razão válida para que a P4BIT os mantenha, os dados pessoais em cópia física serão destruídos como resíduo confidencial, e aqueles mantidos eletronicamente serão excluídos dos sistemas da P4BIT e de terceiros contratados.

Hipóteses de investigação em curso, processos administrativos e judiciais são razões válidas para manutenção dos registros, e independentemente de consentimento, os períodos de armazenamento indicados acima poderão ser prorrogados.

Exceto nas hipóteses acima indicadas, caso a P4BIT tenha o interesse em estender o prazo de armazenamento, os titulares dos dados pessoais deverão ser notificados por escrito, com antecedência razoável da data de término do período de retenção. Se o titular dos registros optar por exercer seu direito de eliminação dessas informações, os dados pessoais serão descartados imediatamente pela P4BIT, exceto em hipóteses de cumprimento de obrigação legal ou regulatória.

Os dados recebidos pelos clientes da P4BIT serão descartados de acordo com o Service Level Agreement (“SLA”) acordado. Na ausência de uma definição, o prazo a ser considerado será de 60 (sessenta) dias após a prestação dos serviços e entrega da notificação de eliminação dos dados.

2.3.8. Eliminação de Dados

A P4BIT e os seus colaboradores realizam regularmente a revisão de todos os dados, sejam eles mantidos eletronicamente ou em papel, para decidir eliminar ou excluir quaisquer dados, uma vez que a finalidade para a qual esses documentos foram criados já não é mais relevante.

Uma vez tomada a decisão de eliminar de acordo com o calendário de retenção, os dados são excluídos, triturados ou destruídos, tendo em atenção se o dado está em forma papel ou em formato eletrônico, dependendo da sua forma e tendo em conta sempre o grau equivalente ao seu valor para os outros e ao seu nível de confidencialidade.

O método de destruição varia e depende da natureza do documento. Por exemplo, quaisquer documentos que contenham informações sensíveis ou confidenciais (e dados pessoais particularmente sensíveis) são destruídos como lixo confidencial e estão sujeitos à eliminação eletrônica segura; alguns contratos expirados ou substituídos podem apenas garantir a destruição interna. A seção de eliminação de documentos abaixo relacionada define o modo de destruição.



Neste contexto, o responsável executa as tarefas e assume as responsabilidades relevantes para a eliminação da informação de forma adequada. O processo específico de eliminação ou destruição deve ser realizado por um colaborador da equipe de proteção de dados.

Existem controles apropriados que impedem a perda permanente das informações essenciais da empresa como resultado da eliminação maliciosa ou não intencional de informações, esses controles são descritos nas Políticas de Segurança da Informação.

A Equipe de Proteção de Dados documenta e provê totalmente o processo de eliminação. Os requisitos legais aplicáveis para a eliminação de informações, particularmente os requisitos sob as leis de proteção de dados aplicáveis que devem ser integralmente observados.

2.3.9. Método de Eliminação

Os documentos de Nível I são aqueles que contêm informações da mais alta segurança e confidencialidade e aquelas que incluem dados pessoais e dados dos clientes. Esses documentos devem ser eliminados como lixo confidencial (triturado transversalmente e incinerado) e sujeitos a uma eliminação eletrônica segura. A destruição dos documentos deve incluir prova de destruição.

Os documentos de Nível II são documentos proprietários que contêm informações confidenciais, como nomes, assinaturas e endereços de terceiros ou que podem ser usados por terceiros para cometer fraudes, mas que não contêm dados pessoais. Os documentos devem ser cortados transversalmente e depois colocados em lixeiras trancadas para serem recolhidos por uma empresa de eliminação aprovada, e os documentos eletrônicos estarão sujeitos à eliminação eletrônica segura.

Documentos de Nível III são aqueles que não contêm informações confidenciais ou dados pessoais. Esses devem ser triturados ou descartados através de uma empresa de reciclagem e incluir, entre outras coisas, anúncios, catálogos, panfletos e boletins informativos. A destruição dos documentos não necessita incluir prova de destruição.

2.3.10. Backup dos dados durante o período de retenção

É considerada a possibilidade de que os meios de dados usados para backup se desgastem. Se forem escolhidos meios de backup eletrônicos, todos os procedimentos e sistemas que garantem o acesso à informação, durante o período de retenção, também serão guardados de maneira a proteger as informações contra perdas, como resultado de futuras mudanças tecnológicas. A responsabilidade pelo armazenamento é da equipe de proteção de dados.



2.3.11. Contato

As solicitações recebidas do titular de registros, para exercer seus direitos durante todo o período de tratamento, serão respondidas da forma e dentro dos prazos exigidos pelas normas aplicáveis.

O titular de dados poderá enviar solicitações, sanar dúvidas e obter mais informações sobre esta Política de Retenção e Descarte de Dados Pessoais através do contato com o encarregado dos dados, o qual poderá ser contatado através do e-mail: contato@p4bit.com.br.

O titular deverá indicar claramente seu nome completo, inserir uma cópia de um documento de identificação e indicar o endereço para o qual a resposta deve ser enviada.

2.4. Política Anticorrupção

2.4.1. Objetivo

Esta Política Anticorrupção (“Política”) tem como objetivo estabelecer as diretrizes gerais sobre práticas de combate à corrupção adotadas pela empresa, em atendimento aos requisitos da legis existentes, em especial à Lei Anticorrupção Brasileira, Lei nº 12.846/13 (“Lei Anticorrupção”), de forma a garantir que durante a condução dos negócios sejam adotados os mais elevados padrões de integridade, equidade, legalidade, transparência e responsabilidade corporativa.

2.4.2. Abrangência

Esta Política aplica-se à P4BIT, bem como a todos os colaboradores, diretores, clientes, parceiros, fornecedores, representantes e terceiros, direta ou indiretamente relacionados com a P4BIT.

2.4.3. Conceitos básico e definições

- **Administração Pública:** é o conjunto de órgãos, entidades e agentes públicos responsáveis por gerir os interesses da sociedade e executar as políticas e serviços públicos em nome do Estado. A administração Pública subdivide-se em Administração Direta (União, Estados, Distrito Federal e Municípios) e indireta (autarquias, fundações públicas, empresas públicas, sociedades de economia mista e eventuais outras constituições de descentralização administrativa).
- **Agentes Públicos:** pessoa que exerce função pública, de forma temporária ou



permanente, ou que trabalhe para empresa prestadora de serviço contratada ou conveniada para a execução de atividade típica da Administração Pública; dirigentes de partido político, seus empregados ou outras pessoas que atuem para ou em nome de um partido político ou candidato a cargo político; e pessoas que trabalham em organizações públicas internacionais.

- **Clientes:** toda pessoa física ou jurídica que contrate os serviços da P4BIT.
- **Colaboradores:** todos os contratados/empregados da empresa, incluindo diretores, gerentes, coordenadores, especialistas, analistas, vendedores, prepostos, trabalhadores com contrato temporário, estagiários, menores aprendizes.
- **Vantagem Indevida:** “qualquer Item de Valor”, não necessariamente econômico, que é oferecida com a intenção de receber favorecimentos em troca.
- **Parceiros Comerciais:** empresas que realizam parceria, fornecedores e representantes que trabalhem junto da P4BIT para atingirem objetivos comerciais.
- **Licitação:** é o procedimento administrativo formal que se estabelece de forma prévia às contratações de serviços, aquisições de produtos, ou até mesmo para registrar preços para contratações futuras da Administração Pública.
- **Lei Anticorrupção nº 12.846/13:** Trata-se de uma Lei federal sobre a responsabilização objetiva, administrativa e civil, de pessoas jurídicas pela prática de atos de corrupção contra a administração pública nacional e estrangeira, incluindo fraudes em licitações e contratos públicos.
- **Lavagem de dinheiro:** ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal.
- **Pessoas Politicamente Expostas:** todas as pessoas que desempenham ou tenham desempenhado nos últimos 5 anos, cargos, empregos ou funções públicas relevantes no Brasil ou em países estrangeiros.

2.4.4. Lei Anticorrupção (Lei nº 12.846/13)

A Lei nº 12.846/13 (“Lei Anticorrupção”) dispõe sobre a responsabilização objetiva administrativa e civil de pessoas jurídicas pela prática de atos lesivos contra a administração pública, nacional ou estrangeira. A Lei foi criada com o objetivo de coibir e punir práticas de corrupção em empresas públicas e privadas, visando promover uma cultura de integridade e transparência no ambiente empresarial.



Sabemos que a implementação da Lei Anticorrupção é uma medida fundamental na prevenção de práticas ilícitas na P4BIT. Desta forma, para garantir a eficácia da lei, criamos um programa de compliance abrangente, com políticas essenciais, inserindo todos os colaboradores e adotando medidas de monitoramento e transparência nas relações comerciais.

A P4BIT realiza análise de risco, identificando possíveis áreas de vulnerabilidade e estabelecendo medidas de mitigação. É importante destacar que a implementação da Lei Anticorrupção não se limita ao combate dos atos de corrupção, mas também deve envolver medidas preventivas, de investigação e de tratamento de denúncias de práticas ilícitas, conforme veremos a seguir.

2.4.5. Medidas de prevenção à corrupção

Com o objetivo de fortalecer cada vez mais e disseminar a cultura anticorrupção dentro da P4BIT, realizamos o monitoramento e revisão periódicos das regras e mecanismos de prevenção à corrupção implementadas pela empresa.

2.4.6. Relacionamento com Parceiros

A seleção de parceiros pela P4BIT será sempre realizada com imparcialidade e transparência, com base em critérios técnicos, profissionais e éticos que impossibilitem contratações pautadas na defesa de interesses pessoais. Por isso, a contratação de qualquer Parceiro deverá ser obrigatoriamente precedida pelo processo de avaliação prévia.

Os colaboradores devem tomar todas as medidas necessárias para observar o devido processo de avaliação prévia e contratação, certificando-se que os Parceiros selecionados seguem os mesmos padrões éticos adotados pela P4BIT. Sendo assim, no processo de avaliação prévia dos Parceiros, deverá ser observada a existência de possíveis sinais de alerta, como os descritos abaixo:

- **Quanto à reputação:** quando o Parceiro: (i) tem interesse econômico que aparenta ser contrário ou incompatível com a sua contribuição a P4BIT; (ii) está envolvido em atividades ilícitas; (iii) é associado ou conhecido pelo uso de empresas de fachada; (iv) fornece declarações ou informações falsas, inconsistentes incompletas ou imprecisas ou se recusar a atender solicitações razoáveis do processo de avaliação e diligência; e (v) requer confidencialidade no que se refere à sua identidade, beneficiários finais ou representantes, sem justificativa razoável.
- **Quanto à qualificação:** quando o Parceiro: (i) é um Agente Público, Pessoa Politicamente Exposta ou Parente Próximo destes; (ii) é recomendado ou



exigido por um Agente Público ou por quem tenha, direta ou indiretamente, qualquer relação de interesse com Agente Público ou Pessoa Politicamente Exposta; e (iii) não apresente as instalações ou qualificações para a execução do trabalho para o qual seria contratado.

- **Quanto à contratação:** quando o Parceiro: (i) se recusa a firmar contrato por escrito; (ii) se recusa a fornecer declarações no que se refere à conformidade; (iii) se recusa a concordar com controles internos; (iv) requer remuneração em um nível substancialmente superior ao de mercado; e (v) solicita que o contrato não descreva com veracidade os serviços que serão fornecidos.
- **Quanto ao pagamento:** Parceiro que: (i) solicita pagamentos incomuns, pagamentos adiantados, comissões fora do mercado ou que sejam pagas fora do país ou para um terceiro; (ii) solicita pagamentos vagos ou indefinidos; e (iii) solicita pagamento sem documentação correta ou para um trabalho que não pode ser comprovado;

Todo relacionamento da P4BIT com qualquer Parceiro deverá ser obrigatoriamente precedido de formalização de contrato, por escrito, nos termos e condições previamente aprovados pelo Departamentos Jurídico.

Na celebração de contrato com qualquer Parceiro, deve-se exigir a assinatura do termo de anuência e ciência das políticas adotadas pela P4BIT, declarando ter amplo conhecimento do conteúdo de tais documentos, comprometendo-se a respeitá-los, bem como a fazer com que seus empregados e contratados os respeitem.

Por fim, todo e qualquer pagamento e transação realizada a título de remuneração, comissão, honorários ou qualquer outra forma de desembolso em favor de Parceiros, ainda que por atividades já desempenhadas, somente poderá ser efetuado pelo Departamento Financeiro, após a aprovação e formalização do respectivo contrato e devem ser cuidadosamente registrados com precisão nas contas da P4BIT, indicando o destinatário e a natureza do pagamento.

2.4.7. Relacionamento com Agentes Públicos

A P4BIT preocupa-se que a interação entre os Colaboradores e Agentes Públicos ou Pessoas Politicamente Expostas ocorra de forma ética, leal, transparente e de acordo com todas as leis, regulamentos e melhores práticas aplicáveis, em todos os casos de fiscalizações e qualquer outro contato em decorrência do negócio da P4BIT.

A realização de reuniões com Agentes Públicos e Pessoas Politicamente Expostas, na discussão de contratos públicos, fiscalizações e outros, deverá ser precedida de solicitação formal, enviada por e-mail ou protocolada no órgão correspondente. As solicitações deverão incluir, no mínimo, as seguintes informações:



- Sugestão de data, horário e local;
- A identidade dos Colaboradores que comparecerão à audiência ou à reunião;
- O assunto que será tratado; e
- Se cabível, o documento que será discutido.

Cabe salientar, que é ilegal oferecer, prometer, pagar ou autorizar o pagamento de qualquer coisa de valor a qualquer Agente Público, com o objetivo de obter vantagem indevida.

Desta forma, todos os Colaboradores e Parceiros da P4BIT deverão reportar imediatamente ao Departamento Jurídico sobre toda e qualquer interação que considerem fora dos padrões éticos e de boa conduta adotados.

2.4.8. Obstáculos à Investigação ou Fiscalização

De acordo com a Lei Anticorrupção, também é ilegal dificultar atividades de investigação ou fiscalização que, eventualmente, estejam sendo realizadas por órgãos, entidades ou agentes públicos, incluindo agências reguladoras e órgãos de fiscalização do sistema financeiro nacional. Exemplos típicos de práticas que podem levantar suspeitas de corrupção e que são proibidas a todos os colaboradores da P4BIT são:

- **Pagamento de propina:** oferecer ou pagar qualquer coisa de valor a agentes públicos que estejam avaliando a necessidade de investigar ou já estejam investigando a empresa;
- **Embaraço à fiscalização:** realizar ações ou omissões que impeçam ou dificultem o acesso de autoridade fiscalizadora à informações ou documentos que existam e estejam de posse das pessoas sujeitas à legislação ou tenham sido solicitados por essa autoridade.

Desta forma, orientamos toda a nossa equipe a melhores práticas, de forma a cooperar com as autoridades públicas durante toda investigação ou fiscalização, garantindo o acesso aos documentos, informações e dados necessários, bem como, evitando a destruição, ocultação ou adulteração de documentos e informações relevantes para a investigação.

2.4.9. Medidas de combate à corrupção

- **Anticorrupção**
 - Embora a corrupção possa ocorrer em qualquer negócio, inclusive nos celebrados com empresas privadas e pessoas físicas, o risco de corrupção é particularmente mais alto e grave quando há interação com Agentes Públicos. Os colaboradores da P4BIT devem sempre se posicionar contra



atos de Corrupção, ainda que a proposta seja realizada por um Agente Público ou por um cliente. Nesses casos, a solicitação deve ser submetida imediatamente ao Departamento Jurídico para assistência e orientação sobre como proceder ou reportar através do Canal de Denúncias para a apuração pertinente.

- Independentemente de com quem se esteja negociando, os Colaboradores devem sempre tomar decisões com base em fatores comerciais legítimos, como preço, qualidade e serviço, entre outros fatores essenciais à livre concorrência e, ao mesmo tempo, devem manter a ética, integridade e transparência da P4BIT em suas negociações com o mercado com o intuito de efetivar contratos e transações idôneos.
- **Pagamentos de Facilitação**
 - Não é permitido aos Colaboradores e Parceiros, que atuem em nome da P4BIT, a realização de pagamentos de facilitação.
 - São considerados pagamentos de facilitação aqueles não vultosos realizados a uma empresa, indivíduo ou agentes públicos, com o objetivo de tentar obter vantagem, agilizar um processo ou obter um benefício que não seria possível obter de outra forma. Todos os Colaboradores e Parceiros estão individualmente obrigados a cumprir as regras previstas nesta Política, no que for cabível, e nas demais políticas internas da P4BIT.
- **Presentes, Brindes, Entretenimento e Hospitalidade**
 - Na P4BIT, o fornecimento ou recebimento de presentes, brindes, hospitalidade ou entretenimento, não devem ter relevância na tomada de decisões corporativas. É permitido o oferecimento de brindes que exibam o nome ou logotipo da P4BIT com o propósito de divulgar o nome e a marca. Os brindes destinam-se a parceiros, clientes e demais pessoas que possuam relacionamento profissional com os Colaboradores. Os brindes não devem constituir forma de presentear, retribuir ou prestar satisfação de relacionamento estritamente pessoal.
 - Os Colaboradores deverão sempre agir no melhor interesse da P4BIT e de seus clientes, devendo evitar qualquer atividade que possa criar um conflito de interesses real ou que seja percebido como ato impróprio às relações dos negócios. As formas legítimas de hospitalidade serão permitidas se o objeto for relacionado aos negócios da P4BIT.
 - Havendo dúvida quanto ao tipo de Brinde, Presente, Entretenimento ou Hospitalidade que possa ser recebido ou oferecido no âmbito das relações empresariais e quanto aos agentes públicos, em situações específicas não mencionadas nesta Política ou no Manual de Ética e Conduta da empresa,



deverá o Colaborador consultar a Diretoria da P4BIT.

- **Contribuições Políticas**

- Os colaboradores não devem prometer, oferecer, autorizar ou dar, direta ou indiretamente, qualquer tipo de contribuição política, para partidos políticos ou para candidatos a cargos públicos com os recursos ou em nome da P4BIT. São consideradas contribuições políticas não só as contribuições monetárias, mas também a disponibilização de meios de transporte para candidatos e suas equipes, o oferecimento de espaços para reuniões relacionadas à campanha eleitoral, o pagamento de gráficas para impressão de material de divulgação ou qualquer outra facilidade que colabore para algum Partido e/ou candidato.
- Esta Política não visa impedir que os colaboradores da P4BIT participem de processo político ou que façam contribuições políticas pessoais. Entretanto, caso desejem fazê-lo, os colaboradores não devem relacionar suas próprias contribuições políticas, de qualquer maneira, à P4BIT e/ou realizar ou permitir que se realize qualquer divulgação que vincule o ato de contribuição à empresa.

- **Patrocínio ou Doações Benéficas**

- Toda e qualquer doação benéfica que vise o apoio a entidades filantrópicas e patrocínio que vise desenvolvimento cultural, esportivo e outros de mesma natureza será permitida, desde que observe estritamente os procedimentos específicos da P4BIT sobre o tema e quaisquer leis e regulamentações aplicáveis em vigor, bem como, que não seja usado como forma de influenciar decisões comerciais de maneira imprópria.
- A P4BIT deve certificar-se de que doações benéficas e patrocínios não sejam usados para promover pagamentos ilícitos e deve conduzir uma due diligence adequada, para evitar que, por exemplo, uma instituição de caridade que venha a ser destinatária atue como um canal para custear atividades ilícitas, em violação a esta Política Anticorrupção ou a quaisquer leis ou regulamentações de combate à corrupção aplicáveis.
- Serão considerados patrocínios toda e qualquer contribuição, em espécie, produtos ou serviços da P4BIT, para uma ação organizada por um parceiro com o objetivo de efetuar propaganda ou divulgação da marca da empresa.
- Os colaboradores responsáveis por patrocínio devem assegurar que tais atividades sejam realizadas de forma transparente, por meio de um acordo escrito para fins comerciais legítimos e de acordo com a contrapartida firmada com o proponente do evento.
- Com relação às doações benéficas, para que não haja questões de não



conformidade com a Legislação Anticorrupção, os Colaboradores poderão realizá-las apenas quando: sejam permitidas pelas leis locais; sejam feitas depois da condução de uma pesquisa razoável que indique que o beneficiário proposto não é associado direta ou indiretamente a um Agente Público; sejam feitas para instituições beneficentes registradas e de boa reputação; não sejam feitas com o objetivo de obter ou reter alguma vantagem ou favorecimento de negócio inadequado; não gerem dependência para a continuidade da entidade beneficiada; os objetivos da entidade beneficiada sejam claramente descritos e alinhados com os valores da P4BIT; a entidade beneficiada formalmente declare como os recursos doados serão utilizados; sejam previamente e formalmente aprovadas; a entidade beneficiada se comprometa, em contrato a prestar contas da utilização dos recursos e a transferência de fundos só possa ser feita para conta bancária em nome da instituição beneficiada. O Colaborador não poderá realizar quaisquer doações ou patrocínios utilizando-se dos recursos da empresa, sem a expressa autorização da Diretoria.

- **Solicitação e Extorsão**

- Caso os Colaboradores venham a se encontrar em uma situação em que acreditem estar em perigo imediato, em que a vida ou segurança de um Colaborador esteja em risco, e sejam compelidos a fazer um pagamento ou a realizar qualquer ato que de alguma forma viole as disposições desta Política, mesmo que os colaboradores não sejam capazes de entrar em contato com o Departamento Jurídico com antecedência, deve primeiro considerar a sua segurança.
- Se forem efetuados pagamentos mediante tais circunstâncias, os Colaboradores devem comunicar imediatamente as circunstâncias e os detalhes do pagamento ao Departamento Jurídico e garantir que tais informações sejam registradas com precisão nos livros e registros da P4BIT. Registrar ocorrência, quando tratar-se de fato cometido enquanto crime. Eventualmente poderão surgir situações não descritas na presente Política ou no Manual de Ética, nesses casos, recomenda-se, aos Colaboradores e Parceiros contatarem o Departamento Jurídico para sanar eventuais dúvidas.

2.4.10. Responsabilidades e atribuições

- **Colaboradores**

- São Responsabilidades e Atribuições dos Colaboradores:



- Conhecer e cumprir todas as diretrizes do Manual de Ética da P4BIT e desta Política;
 - Colaborar com as investigações internas ou de órgãos fiscalizadores externos, sempre sob o assessoramento do Departamento Jurídico e outras áreas relacionadas, conforme aplicável;
 - Reportar ao Departamento Jurídico caso presencie ou saiba de qualquer situação de risco ou suspeita de Corrupção, Fraude, Suborno ou outra violação ao Manual de Ética e demais políticas;
 - Interromper prontamente quaisquer atividades em desacordo com esta Política, assim que forem detectadas;
 - Manter adequadamente os registros financeiros, contábeis e controles internos de sua responsabilidade.
- **Jurídico**
 - São Responsabilidades e Atribuições do Departamento Jurídico:
 - Orientar os Colaboradores sobre esta Política;
 - Mapear os riscos relacionados ao descumprimento da Lei Anticorrupção e ao Manual de Ética da empresa e propor medidas de controle;
 - Receber e analisar as denúncias de violação ao Manual de Ética e a esta Política;
 - Monitorar o cumprimento desta Política;
 - Reportar situações de descumprimento desta Política e do Manual de Ética.
 - Estabelecer cláusulas Anticorrupção e de cumprimento do Manual de Ética a ser incluída nos contratos com Terceiros;
 - Realizar due diligence em relação a todas as partes interessadas, incluindo fornecedores, parceiros de negócios e terceiros, para garantir que eles atendam aos padrões éticos e legais exigidos.
- **Financeiro**
 - São Responsabilidades e Atribuições do Departamento Financeiro:
 - Implementação e observância da presente Política e da legislação vigente sobre o assunto.
 - Observância da legalidade e dos riscos relativos às operações financeiras realizadas pela P4BIT.
 - Implementar políticas e procedimentos claros e rigorosos para orientar as atividades financeiras e evitar conflitos de interesse e outras práticas corruptas.
 - Fornecer treinamento e conscientização adequados aos



funcionários e partes interessadas sobre a importância da prevenção da corrupção e as consequências legais e financeiras de práticas corruptas.

- Monitorar continuamente as atividades financeiras e realizar auditorias regulares para identificar qualquer atividade suspeita ou práticas corruptas.
- Estar preparado para responder prontamente a qualquer suspeita de corrupção ou atividade ilegal, investigando imediatamente e tomando as medidas corretivas necessárias.

- **Terceiros**

- São Responsabilidades e Atribuições de Terceiros:

- Observar e cumprir as diretrizes da Lei Anticorrupção e da Declaração de Conformidade à Legislação e Ética da P4BIT;
 - Reportar ao Departamento Jurídico caso presencie ou saiba de qualquer situação de risco ou suspeita de Corrupção, Fraude, Suborno ou outra violação ao Manual de Ética e demais políticas.

2.4.11. Treinamento

A P4BIT dissemina as diretrizes desta Política e do seu Programa de Integridade por meio de comunicações e treinamentos definidos pelo Departamento Jurídico. Todos os colaboradores devem, obrigatoriamente, participar dos treinamentos quando convocados.

Além disso, a P4BIT promoverá anualmente treinamentos, voltados aos colaboradores, com a finalidade de capacitá-los para o reconhecimento de situações que possam colocar a empresa ao risco de exposição a questionamentos ou penalidades por atos de corrupção e a prevenção e combate de atos dessa natureza dentro da P4BIT, em suas interações com terceiros e agentes públicos. A presença dos colaboradores nos treinamentos é obrigatória.

Em caso de alterações significativas à atual versão da Política, o Departamento Jurídico da P4BIT promoverá novos treinamentos voltados a todos os colaboradores.

Se, após qualquer treinamento ainda persistirem dúvidas, os Colaboradores e parceiros deverão entrar em contato com o Departamento Jurídico, que poderá esclarecê-los e recomendar o modo mais apropriado de agir em situações que possam expor a P4BIT a questionamentos ou penalidades por práticas lesivas à administração pública.



2.4.12. Auditoria Interna

A P4BIT realizará periodicamente auditorias internas para avaliar o cumprimento às Leis Anticorrupção e esta Política.

A Auditoria Interna tem como principal função o exame dos processos internos, verificando a adequação e validação dos processos, das informações e registros, recomendando melhorias quando necessário.

2.4.13. Diretrizes e Regras

Algumas regras gerais de prevenção à corrupção e ao suborno em conformidade com a Lei Anticorrupção e Manual de Ética da P4BIT, são aplicadas a todos os colaboradores ou pessoas que interagem com a empresa. Desta forma, é proibido a estes:

- Dar, oferecer, prometer ou autorizar que se dê vantagem indevida a agentes públicos ou a terceira pessoa a ele relacionada, diretamente ou por meio de intermediários;
- Dar, oferecer, prometer ou autorizar que se dê vantagem indevida para Terceiros a fim de garantir benefícios para a P4BIT ou à terceiro;
- Financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos na legislação aplicável;
- Utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
- Dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos ou intervir em sua atuação;
- Manipular ou fraudar licitação pública ou contratos celebrados com a administração pública;
- Dar, oferecer, prometer ou autorizar que se dê pagamentos de facilitação que não são exigidos ou previstos em lei ou regulamento, para iniciar ou acelerar um processo ou procedimento que é de responsabilidade do agente público.

Ressalta-se que não há negócio ou resultado que justifique o Suborno e/ou Corrupção. Todo colaborador ou indivíduo que interage com a empresa deve rejeitar qualquer oferta de Vantagem Indevida, Suborno ou Corrupção e evitar qualquer conduta que possa ser interpretada como sendo imprópria ou não condizente com os padrões estabelecidos no Manual de Ética da empresa. A P4BIT não tolera que seus Colaboradores e Terceiros compactuem com tais práticas.



2.4.14. Sanções aplicáveis

O colaborador que descumprir quaisquer diretrizes ou medidas estabelecidas nesta Política estará sujeito à aplicação de sanções disciplinares, responsabilização civil ou até mesmo criminal, sem prejuízo de outras penalidades ou medidas cabíveis de acordo com a legislação vigente.

2.4.15. Canal de denúncia

O canal de denúncia é gerenciado pela P4BIT, responsável pelo processamento das denúncias recebidas e encaminhamento para apuração do Departamento Jurídico. Toda e qualquer denúncia poderá ser feita anonimamente, sendo a identidade do denunciante protegida durante todo o processo de apuração se ele assim o desejar.

As denúncias podem ser feitas por meio do nosso Canal de Denúncia, através do e-mail: compliance@p4bit.com.

2.5. Política de prevenção e combate à lavagem de dinheiro

2.5.1. Objetivo

A Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo (“Política”) visa definir as diretrizes, regras e procedimentos, a fim de promover a adequação das atividades operacionais com as exigências legais e regulamentares, assim como melhores práticas pertinentes aos crimes de Lavagem de Dinheiro e Financiamento do Terrorismo, além de demais crimes envolvendo simulação ou ocultação de recursos financeiros.

A Política tem ainda como objetivo a disseminação da cultura de Prevenção e Combate à Lavagem de Dinheiro, consoante as práticas de governança corporativa, visando assegurar um completo e eficaz conhecimento e monitoramento de ações consideradas suspeitas.

2.5.2. Abrangência

Esta Política aplica-se à P4BIT, bem como a todos os colaboradores, diretores, clientes, parceiros, fornecedores, representantes e terceiros, direta ou indiretamente relacionados com a P4BIT.

2.5.3. Conceitos básicos e definições

- **Lavagem de Dinheiro:** Para fins desta Política, consoante definição do artigo 1º da Lei nº 9.613/98, os atos de lavagem de dinheiro se referem à ocultação ou



dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. Logo, o agente simula a obtenção de recursos ilícitos, de forma que pareçam lícitos, a fim de utilizá-los sem comprometer a sua reputação. A lavagem de dinheiro ocorre em três etapas: (i) Colocação: A colocação se realiza por meio de depósitos em bancos ou instituições financeiras, compra de instrumentos negociáveis ou de bens no comércio ou em operações nas quais se admite dinheiro em espécie; (ii) Ocultação: A segunda etapa do processo consiste em dificultar o rastreamento contábil das operações e recursos; e (iii) Integração: nesta última etapa, os ativos são incorporados formalmente ao sistema econômico.

- **Financiamento do Terrorismo:** Financiamento ao terrorismo é o processo de prover recursos financeiros ou materiais para apoiar atividades terroristas. Isso pode incluir o fornecimento de dinheiro, armas, explosivos, veículos, equipamentos de comunicação ou qualquer outro tipo de suporte financeiro ou material que possa ser utilizado para financiar e executar atividades terroristas. Trata-se de uma atividade criminosa grave, que ajuda a manter organizações terroristas em operação e permite que elas realizem atos de violência, atentados e outras atividades ilegais.
- **Compliance:** tem origem no verbo inglês “to comply”, significa cumprir, obedecer, estar de acordo. Define-se Compliance como seguir as leis, normas e procedimentos internos das organizações, além de parcerias éticas, seja com o setor público ou privado e seus fornecedores.
- **Pessoa Politicamente Exposta:** são pessoas naturais que ocupam ou tenham ocupado, nos últimos 5 (cinco) anos, empregos ou funções públicas relevantes, assim como funções relevantes em organizações internacionais.
- **COAF - Conselho de Controle de Atividades Financeiras:** Conselho criado no âmbito do Ministério da Fazenda com a finalidade de disciplinar, aplicar penas administrativas, receber, examinar e identificar as ocorrências suspeitas de atividades ilícitas previstas na Lei nº 9.613/1998, sem prejuízo da competência de outros órgãos e entidades.
- **Colaboradores:** qualquer pessoa física ou jurídica que possua vínculo contratual ou empregatício com a P4BIT para prestação de serviços, abrangendo inclusive estagiários, empregados temporários, empregados efetivos, prestadores de serviços e menores aprendizes.



2.5.4. Áreas responsáveis e atribuições

O cumprimento da legislação vigente sobre as práticas de Lavagem de Dinheiro e ao Financiamento do Terrorismo, bem como, da presente Política, é de responsabilidade da P4BIT. A divisão de responsabilidades na estrutura de governança, seguirá da seguinte maneira:

- **Diretoria Financeira:** É incumbência da Diretoria Financeira a prevenção e o combate dos crimes de Lavagem de Dinheiro e de Financiamento do Terrorismo e a implementação e observância da presente Política e da legislação vigente sobre o assunto. É responsabilidade da Diretoria Financeira a observância da legalidade e dos riscos relativos às operações financeiras realizadas pela P4BIT, bem como garantir a consonância das diretrizes com as determinações dos órgãos reguladores. Caberá ainda à Diretoria Financeira da P4BIT garantir as comunicações ao COAF.
- **Diretoria Operacional:** É incumbência da Diretoria Operacional a implantação e gestão de controles visando a mitigação dos riscos das operações da P4BIT relativos ao Financiamento do Terrorismo e Lavagem de Dinheiro, e a implantação e gestão de processos de monitoramento visando a detecção de transações suspeitas ou atípicas relacionadas à atos, procedimentos e registros de operações que possam configurar indícios de Financiamento ao Terrorismo ou de Lavagem de Dinheiro.
- **Departamento Jurídico/Área de Compliance:** Compete ao Departamento Jurídico analisar os contratos celebrados pela P4BIT com clientes, fornecedores e terceiros, bem como identificar a magnitude dos impactos jurídicos tendo em vista o risco de Lavagem de Dinheiro e de Financiamento do Terrorismo. Também compete ao Departamento Jurídico prestar apoio sobre a orientação, a indicação e a composição do rol mantido pela P4BIT sobre as pessoas politicamente expostas (PEP). O Departamento Jurídico é responsável pela Área de Compliance, devendo assegurar a conformidade das políticas internas e das atividades preventivas da P4BIT com a legislação vigente sobre as práticas de Lavagem de Dinheiro e de Financiamento do Terrorismo. A Área de Compliance possui algumas atribuições para efetivar o cumprimento desta Política, incluindo, mas não se limitando a:
 - Implementar as diretrizes da presente Política;
 - Apurar denúncias de violação aos termos dispostos nesta Política e propor a adoção das medidas disciplinares cabíveis;
 - Identificar, qualificar e classificar os clientes;
 - Realizar anualmente a validação de empresas parceiras;



- Avaliar novos produtos a fim de verificar possíveis riscos de lavagem de dinheiro e financiamento do terrorismo a eles relacionados;
 - Avaliar as demandas sobre novas tecnologias que tenham sido consideradas pela primeira linha de defesa como de risco de lavagem de dinheiro e/ou financiamento de terrorismo;
 - Elaborar parecer específico de risco reputacional, lavagem de dinheiro e financiamento do terrorismo, de acordo com background check realizado por meio de ferramentas específicas a respeito das pessoas físicas e jurídicas que celebraram contratos comerciais com a P4BIT.
- **Gestores:** Consideram-se Gestores, para fins desta Política, todos os Diretores, Gerentes, Coordenadores e Supervisores da P4BIT. Os Gestores são responsáveis pela disseminação desta Política e acompanhamento de seus subordinados, certificando-se de que eles estejam em conformidade com a regulamentação, normas e procedimentos de prevenção e combate à Lavagem de Dinheiro e Financiamento ao Terrorismo.
 - **Setor de Recursos Humanos:** O Setor de Recursos Humanos é responsável por viabilizar, em conjunto com o Departamento Jurídico e Controles Internos, programas de treinamento para assegurar que todos os colaboradores estejam devidamente orientados e atualizados quanto às suas obrigações e responsabilidades perante as condições descritas nesta Política e nas legislações aplicáveis no tocante à Lavagem de Dinheiro e Financiamento ao Terrorismo.
 - **Demais Colaboradores:** Todos os colaboradores da P4BIT são responsáveis pelo cumprimento das regras previstas nesta Política, bem como pela disseminação dos valores e princípios da empresa e pela contribuição da manutenção de um ambiente de trabalho íntegro. Os Colaboradores devem ser diligentes no monitoramento e detecção de operações com indícios de Lavagem de Dinheiro e de Financiamento do Terrorismo, seguir a política interna de prevenção e informar a área de Compliance sobre qualquer situação suspeita.

2.5.5. Diretrizes preventivas

A P4BIT adota diversas diretrizes para prevenir a ocorrência de ações de Lavagem de Dinheiro e Financiamento do Terrorismo, dentre as quais:

- Orientamos e capacitamos todos os Colaboradores para que conduzam suas atividades e negócios com integridade, evitando qualquer forma de fraude ou práticas que possam acarretar ou facilitar a Lavagem de Dinheiro;



- As operações realizadas pela P4BIT com terceiros são devidamente documentadas e armazenadas, estando à disposição para a fiscalização dos órgãos reguladores.
- A P4BIT não admite em seus negócios a movimentação de recursos por meio de contas correntes anônimas ou vinculadas a titulares fictícios.
- A P4BIT adota procedimentos de Due Diligence de parceiros comerciais e terceiros, fazemos uma avaliação adequada destes para garantir que não estejam envolvidos em atividades ilegais, bem como a integridade da contratação;
- De acordo com as exigências legais e as melhores práticas do mercado, a P4BIT mantém programas de treinamento e de disseminação de cultura de prevenção à lavagem de dinheiro, de combate ao financiamento do terrorismo e à corrupção.
- Adotamos o procedimento “Conheça seu cliente” (KYC), verificamos a identidade do cliente e a natureza de seus negócios antes de realizar qualquer transação.
- Monitoramos as transações para identificar qualquer atividade suspeita, incluindo transações em grande volume ou incomuns para o cliente.
- Estabelecemos políticas e procedimentos internos e revisamos regularmente estes para garantir que sejam eficazes na prevenção da lavagem de dinheiro.
- Em caso de ações suspeitas, comunicamos imediatamente as autoridades reguladoras.

2.5.6. Procedimento para conhecer os clientes, colaboradores e fornecedores

- **Conheça seu Cliente (Know Your Cliente – KYC):**
A P4BIT capacita seus funcionários para realizarem a coleta, verificação, validação e atualização de informações cadastrais, visando a conhecer os clientes no que se refere a identificação dos riscos de ocorrência de Lavagem de Dinheiro e Financiamento ao Terrorismo. O relacionamento da P4BIT com o seu cliente será sempre norteado pela perspectiva de transparência e integridade de suas atividades, dentro do conceito "Conheça Seu Cliente", e não apenas pelo interesse comercial e/ou rentabilidade que esse cliente possa proporcionar no seu relacionamento com a empresa. Para tanto, a P4BIT realiza as seguintes atividades:
 - Análise cuidadosa dos documentos apresentados pelo cliente;
 - Análise da atividade econômica/capacidade financeira do cliente, quando necessário;



- Manutenção do cadastro do cliente atualizado e verificação de alterações da atividade econômico-financeira, quando necessário;
- Armazenamento e conservação das informações e registros das operações do Cliente;
- Coleta de informações pessoais: a empresa coleta informações pessoais do cliente, como nome, endereço, data de nascimento e número de identificação pessoal.
- Verificação da identidade (pessoa física): a P4BIT verifica a identidade do cliente por meio de documentos de registro e identificação, como carteira de identidade, passaporte ou carteira de motorista.
- Verificação de documentos e registros (pessoa jurídica): a P4BIT verifica a regularidade dos clientes por meio de consultas, tais como, consulta ao CNPJ e Contrato social;
- Avaliação de riscos: a P4BIT avalia os riscos associados ao cliente com base na natureza de seus negócios, e outros fatores relevantes.
- Monitoramento das transações: a P4BIT monitora as transações do cliente para identificar atividades suspeitas, como transações em grande volume ou incomuns para o cliente.
- Revisão periódica: a P4BIT realiza revisões periódicas da informação do cliente para garantir que ela ainda esteja atualizada e precisa.

O objetivo deste item na Política e dos controles relacionados é de estabelecer ações de modo a:

- Assegurar a conformidade com a legislação, normas e regulamentos que disciplinam a prevenção e o combate à Lavagem de Dinheiro e Financiamento ao Terrorismo;
 - Assegurar a conformidade com as ações de Prevenção e Combate à LDFT no estabelecimento de novos relacionamentos e outros controles relacionados;
 - Minimizar riscos operacionais, legais e de reputação aos quais a empresa possa estar sujeita, caso venha a ser utilizada para a prática destes crimes, mediante a adoção de um sistema de monitoramento de transações, procedimentos e controles internos;
 - Identificar e designar, de modo claro, as responsabilidades e atribuições em todos os níveis hierárquicos e operacionais;
- **Conheça seu Colaborador (Know Your Employee – KYE):**
A análise dos colaboradores da P4BIT deve compreender, a fase de recrutamento e seleção de candidatos mediante entrevistas com os recursos humanos e líder da área contratante, análise curricular, pesquisas ligadas a



reputação do candidato no mercado (Serasa, Receita Federal, e Internet) e seus antecedentes criminais.

No ato de contratação, o colaborador assina o Termo de adesão ao Manual de Ética e Conduta e o Termo de Confidencialidade e Sigilo, bem como toma conhecimento das políticas adotadas, a fim de que o colaborador possa estar comprometido com os princípios da P4BIT e preparado para assumir suas funções de acordo com à sua área de atuação. Os colaboradores da P4BIT serão treinados periodicamente em aspectos técnicos do ramo de negócio, Controles Internos, Código de Ética e Conduta Empresarial, Lavagem de Dinheiro, através de treinamentos virtuais e presenciais. Os treinamentos têm por finalidade principal a disseminação da cultura da P4BIT, o constante aprimoramento técnico dos colaboradores, apoiado pelas políticas, procedimentos, melhores práticas de mercado, normas/regulamentações e com as legislações vigentes.

A P4BIT apresentará as normas internas de Prevenção e Combate à Lavagem de Dinheiro e de Financiamento ao Terrorismo, principalmente àqueles que exercerão atividades que envolvam ações fraudulentas ou que atuem em funções de relacionamento com clientes como, área comercial, entre outras.

Considerando a criticidade, a severidade e o efeito lesivo provocado pelos atos ilícitos, bem como os riscos de imagem e reputação cada vez mais relevantes nas atividades, a P4BIT, consciente de seu compromisso, estabelece as diretrizes contra a corrupção, à lavagem de dinheiro e ao financiamento do terrorismo, a serem observadas pelos colaboradores nos diversos relacionamentos e no cotidiano de suas atividades e funções profissionais, conforme segue:

- Abster-se de atos que possam comprometer a reputação e a imagem da instituição, seguindo as melhores regras de conduta, não praticando, não cooperando e repelindo qualquer negócio ou atividade ilícita, dentre eles, a prática de propinas, subornos, extorsão, desvios e corrupção em todas as suas formas, seja nos relacionamentos com o setor privado e/ou com o setor e agentes públicos, nacionais ou estrangeiros;
- Abster-se de comentar qualquer informação ou emitir opinião que possa ser utilizada para a realização ou participação em negócios ou atividades escusas ou questionáveis;
- Abster-se de oferecer sugestões ou aconselhamentos de ordem pessoal ou financeira que possam dar a entender disposição em colaborar com



negócios ou atividades que busquem escapar de restrições, normas, leis e regras impostas por qualquer autoridade ou regulamento;

- Manter-se vigilante no sentido de identificar e repelir as tentativas de uso da P4BIT para negócios ou práticas ilícitas, fraudes ou crimes de qualquer natureza, principalmente os relacionados a suborno, corrupção, lavagem de dinheiro e financiamento ao terrorismo;
- Não utilizar o cargo ou o nome da P4BIT para obtenção de qualquer vantagem financeira ou material, para si ou para terceiros, ou mesmo de negócios ou procedimentos que possam configurar ação ou omissão imprópria no desempenho de suas funções, incluindo práticas de tráfico de influência ou abuso de poder;
- Recusar presentes, vantagens pecuniárias ou materiais, de quem quer que seja, que possam representar relacionamento impróprio ou em prejuízo financeiro ou de reputação para a empresa;
- Manter sigilo sobre as informações internas e de clientes às quais tenha acesso em razão do exercício do cargo ou função;
- Em hipótese alguma fornecer, ceder ou repassar, por qualquer meio ou forma, documentos e informações que estejam protegidos por sigilo bancário ou acordo de confidencialidade;
- Não fornecer, ceder ou repassar, por qualquer meio ou forma, a quem quer que seja, sua senha de uso pessoal para acesso à rede de computadores e a sistemas de informações da instituição;
- Abster-se direta ou indiretamente de, em seu nome e interesse pessoal, firmar, controlar, custodiar, intermediar ou representar interesses de clientes, fornecedores ou terceiros; e
- Zelar pela manutenção e integridade de todo e qualquer documento e registro interno, não permitindo, em hipótese alguma, que eles sejam retirados, alterados ou destruídos, com o propósito de ocultar ou dissimular transação ou procedimento inadequado ou em desacordo com a regulamentação interna ou externa.

A P4BIT assegurará o comprometimento e a dedicação dos colaboradores, promovendo a disseminação de seus valores éticos e diretrizes de prevenção a fraudes e ilícitos, bem como, realizará a avaliação e os monitoramentos preventivos necessários para o combate aos referidos crimes.

- **Conheça seu Fornecedor (Know Your Partner – KYP):**

A P4BIT zela por sua integridade, por isso, só estabelece relacionamento com parceiros que sejam idôneos e que não exerçam nenhuma atividade ilícita.

Diante disso, a P4BIT analisa seus fornecedores com o objetivo de esclarecer



quaisquer dúvidas quanto a seus valores éticos, idoneidade, honestidade e reputação, verificando cuidadosamente quaisquer indícios que possam indicar propensão do parceiro quanto a atos ilícitos. Os procedimentos serão proporcionais aos riscos enfrentados em cada contratação.

O processo de contratação de fornecedores são atividades de suma importância dentro da P4BIT, tanto para observância de questões regulatórias quanto para mitigação de riscos legais e reputacionais. A devida diligência consiste no processo de análise, fundamental para a confirmação dos dados disponibilizados pelos fornecedores em processos de seleção.

A P4BIT entende ser importante trabalhar com fornecedores que tenham sua situação econômico-financeira saudável e que assumam suas responsabilidades legais, regulatórias, trabalhistas, sociais e ambientais.

Desse modo, sempre que houver a contratação de fornecedores que atenderem os critérios de relevância definidos pela área de Compliance, deverá ser realizado o processo de due diligence e a aprovação da respectiva área.

Antes de iniciar suas operações com a P4BIT, o fornecedor deverá fornecer todas as informações cadastrais conforme solicitado durante o processo de contratação. São estabelecidas as seguintes diretrizes de avaliação:

- Análise do perfil do fornecedor a partir das informações que foram disponibilizadas;
- Verificação da identidade da empresa e as informações de contato, incluindo endereço e número de telefone, além de avaliar a reputação da empresa e possíveis históricos de problemas legais ou éticos;
- Avaliação da estabilidade financeira do fornecedor ou parceiro de negócios, para garantir que eles possam cumprir seus compromissos financeiros e que não haja risco de falência ou atraso nos pagamentos;
- Análise do fornecedor quanto à conformidade com as regulamentações e leis aplicáveis, como as leis de proteção de dados, trabalhistas e ambientais, por exemplo;
- Análise dos riscos de segurança associados a um fornecedor, incluindo riscos de cibersegurança, riscos físicos e riscos de terceirização.
- Monitoramento contínuo de fornecedores/parceiros comerciais para detectar quaisquer mudanças que possam afetar seu risco ou conformidade regulatória;
- Estabelecimento de contratos e acordos claros com



fornecedores/parceiros comerciais, especificando os termos e condições do relacionamento comercial e as responsabilidades de cada parte.

2.5.7. Diretrizes de combate

- **Detecção de atos criminosos**

Todo colaborador é um parceiro importante no combate ao cometimento de atos ilícitos. Dessa forma, qualquer colaborador que tiver conhecimento ou suspeitar da ocorrência real ou iminente de Lavagem de Dinheiro ou de Financiamento ao Terrorismo, deverá comunicar imediatamente a Área de Compliance. Aquele que deixar de comunicar suspeitas ou violações que tiver conhecimento, será considerado conivente na violação dos termos desta Política, estando sujeito a medidas disciplinares. A comunicação de referidas condutas será protegida, e não tolerará atos de retaliação contra aquele que fizer as denúncias de ocorrência de Lavagem de Dinheiro ou de Financiamento ao Terrorismo, desde que de boa-fé. Caso existam atos de retaliação em desfavor do denunciante, a Área de Compliance deverá ser imediatamente informada, para fins de investigação e aplicação de medidas disciplinares cabíveis aos indivíduos. Tão logo ciente de suspeitas ou de violações da presente política e da legislação aplicável, a P4BIT comunicará os órgãos necessários sobre a existência de possíveis condutas criminosas.

- **Canal de denúncia**

O canal de denúncia é gerenciado pela P4BIT, responsável pelo processamento das denúncias recebidas e encaminhamento para apuração do Departamento Jurídico. Toda e qualquer denúncia poderá ser feita anonimamente, sendo a identidade do denunciante protegida durante todo o processo de apuração se ele assim o desejar. As denúncias podem ser feitas por meio do nosso Canal de Denúncia, através do e-mail: compliance@p4bit.com.

- **Investigação de Casos Reportados**

A apuração dos fatos relacionados à Lavagem de Dinheiro e ao Financiamento ao Terrorismo será realizada pela Área de Compliance em conjunto com o Diretoria Financeira, por meio de levantamento de documentação, comparação de dados com registros existentes, análise de históricos, dentre outros procedimentos cabíveis, visando, dentre outros, evidenciar o ato ilícito, de maneira a possibilitar a recuperação de eventuais perdas financeiras sofridas pela P4BIT.

Não obstante a comunicação feita juntamente aos órgãos necessários sobre possíveis cometimentos de condutas ilícitas, as investigações internas serão conduzidas de forma independente pela Área de Compliance, que terá plena



autonomia para realizar as diligências aptas à comprovação do ato ilícito. Assim, a Área de Compliance conduzirá todas as investigações com equidade e imparcialidade, respeitando os direitos dos indivíduos e/ou entidades envolvidas, inclusive garantindo a presunção de inocência até a conclusão dos procedimentos de análise.

- **Disciplinares**

Após a análise da denúncia reportada, se constatada a prática de Lavagem de Dinheiro ou de Financiamento ao Terrorismo, a P4BIT fará a devida comunicação aos órgãos competentes e aplicará as medidas disciplinares cabíveis, dentre as quais:

- Demissão: A P4BIT poderá demitir o colaborador que cometeu a Lavagem de Dinheiro.
- Acusações Criminais: Se a lavagem de dinheiro for uma violação da lei criminal, o colaborador pode enfrentar acusações criminais.
- Ações Judiciais: O colaborador poderá sofrer ações judiciais, a fim de ser responsabilizado civilmente pelos danos causados à empresa ou a terceiros.
- Restituição: O colaborador pode ser obrigado a devolver o dinheiro ou bens obtidos ilegalmente.
- Proibição de Contratação Futura: A P4BIT pode proibir o funcionário de ser recontratado no futuro.
- Denúncia às Autoridades: A P4BIT pode denunciar a atividade criminosa às autoridades competentes, como a Polícia ou o Ministério Público.

Fica a critério da P4BIT, por intermédio da Área de Compliance, iniciar ou não a acusação civil e/ou criminal contra os envolvidos no cometimento dos atos ilícitos.

2.5.8. Vigência e revisão

Esta Política foi revisada e aprovada pelo Departamento Jurídico, e possui vigência por prazo indeterminado, podendo ser alterada em casos de modificações nas legislações aplicáveis ou em eventual mudança das práticas de negócios que justifiquem a atualização.

A revisão contempla a reavaliação de todos os riscos envolvidos e abordados nesta Política. Após a revisão e aprovação pelo Departamento Jurídico, esta Política será disponibilizada no site da P4BIT.



2.5.9. Considerações finais

A política de prevenção e combate à Lavagem de Dinheiro e Financiamento do Terrorismo é essencial para proteger a integridade da P4BIT e evitar envolvimento em atividades ilegais. Ao longo da elaboração desta política, foram implementadas medidas eficazes para identificar e mitigar riscos, incluindo a criação de procedimentos de due diligence, monitoramento de transações suspeitas e a implementação de treinamentos para os colaboradores. A P4BIT está preparada para lidar com a complexidade do cenário de risco de lavagem de dinheiro e financiamento do terrorismo e para proteger a empresa contra possíveis consequências negativas. Por fim, para manter o sucesso desta política, é importante continuar aprimorando nossas práticas e revisando periodicamente nossos procedimentos.

2.6. Política de responsabilidade socioambiental

2.6.1. Objetivo

Esta Política de Responsabilidade Socioambiental (“Política”), tem como objetivo estabelecer os princípios e as diretrizes compatíveis com a natureza e complexidade das atividades e serviços da P4BIT, para o desenvolvimento de práticas e ações socioambientais nos negócios e na relação com colaboradores, parceiros comerciais e terceiros.

2.6.2. Abrangência

Esta Política aplica-se à P4BIT, bem como a todos os colaboradores, diretores, clientes, parceiros, fornecedores, representantes e terceiros, direta ou indiretamente relacionados com a P4BIT.

2.6.3. Princípios

Os princípios Socioambientais aplicáveis à P4BIT objetivam orientar suas ações de forma a colaborar com a preservação do meio ambiente, o estabelecimento de um ambiente de trabalho saudável e desenvolvimento da sociedade. São princípios que norteiam a P4BIT nas práticas Socioambientais:

- Boas práticas de Governança Corporativa;
- Valorização das pessoas e respeito aos Direitos Humanos;
- Postura ética e transparente nas relações com os públicos de interesse, repudiando qualquer forma de discriminação ou ilicitude, em conformidade com o Manual de Ética e de Conduta Empresarial da P4BIT e da Política



Anticorrupção;

- Busca pela sustentabilidade nos negócios e nos relacionamentos;
- Respeito e fortalecimento de características econômicas, culturais, sociais e ambientais das comunidades onde estamos inseridos;
- Excelência e qualidade na prestação de serviços;
- Inclusão e educação financeira.

2.6.4. Diretrizes

A P4BIT possui uma Política de Responsabilidade Socioambiental que se baseia em dois pilares: o social e o ambiental. Esses pilares abrangem uma série de temas relevantes que reforçam o compromisso da empresa com o desenvolvimento sustentável e orientam sua gestão:

- **Ambiental:** no intuito de minimizar os impactos ambientais associados às suas atividades, a P4BIT compromete-se a adotar programas de ecoeficiência em suas dependências, otimizar o uso de água, energia e papel, gerenciar adequadamente os resíduos sólidos, inclusive lixo eletrônico, e suas emissões de gases de efeito estufa. Compromete-se, ainda, a induzir boas práticas ambientais na sua cadeia de valor.
- **Social:** como uma empresa socialmente responsável que respeita seus relacionamentos internos e externos e promove os Direitos Humanos, a P4BIT empenha-se em atrair e reter talentos, incentivar a busca pela melhoria da qualidade de vida e desenvolver seus colaboradores, incentivar a diversidade, inclusão e igualdade de gênero. Compromete-se, ainda, a induzir as boas práticas sociais na sua cadeia de valor.

As diretrizes baseadas nos princípios estão descritas a seguir e norteiam nossas ações para a efetiva implementação desta Política. Quanto às diretrizes sociais, a P4BIT se responsabiliza por:

- Adotar normas internas que valorizem a diversidade e a equidade, promovendo o respeito aos direitos humanos;
- Preservar a individualidade e a privacidade dos colaboradores, não admitindo a prática de atos discriminatórios e de assédio, de qualquer natureza, no ambiente de trabalho e em todas as relações;
- Desenvolver a cultura da sustentabilidade, através de processo de educação e comunicação continuados;
- Possibilitar condições de trabalho adequadas ao bem-estar dos colaboradores, considerando os padrões de saúde, segurança operacional e qualidade de vida.



- Implementar as diretrizes desta Política nos processos de gestão da empresa;
- Promover o engajamento de todos os colaboradores com esta Política;
- Estimular o atendimento às necessidades dos clientes, com respeito à diversidade;
- Proporcionar acessibilidade aos usuários dos serviços ofertados;
- Buscar a fidelização de clientes, por meio do desenvolvimento de relacionamentos de longo prazo, pautados na ética, transparência, confiança e na sustentabilidade;
- Repudiar todos e quaisquer aspectos relacionados ao trabalho análogo ao escravo, ao trabalho infantil e à exploração sexual;
- Estabelecer e contemplar critérios socioambientais nos processos de compras e contratação de serviços, além de critérios relacionados à economicidade, ao atendimento à legislação, às especificações de qualidade de produtos e serviços e à confiabilidade nos prazos de entregas.
- Respeitar os valores culturais, sociais e ambientais de todas as comunidades, especialmente onde a P4BIT está inserida;
- Apoiar políticas públicas que visem à redução das desigualdades sociais e econômicas;
- Negócios com empresas e/ou pessoas envolvidas em processos de corrupção e ou financiamento a ações de terrorismo.

Quanto às diretrizes ambientais, a P4BIT se responsabiliza por:

- Estabelecer as diretrizes para a P4BIT obter controle sobre os riscos socioambientais inerentes ao negócio e gerenciá-los de maneira integrada aos demais riscos da empresa;
- Gerenciar riscos socioambientais nas atividades relativas a esta Política, à gestão de pessoas, gestão de resíduos, eficiência energética e relações com fornecedores, parceiros e clientes;
- Avaliar previamente os potenciais impactos socioambientais e reputacionais provenientes de novos serviços;
- Estabelecer procedimentos para adequação do gerenciamento do risco socioambiental às mudanças legais, regulamentares e de mercado.
- Promover a gestão adequada dos resíduos gerados, adotando sempre que possível o processo de reciclagem e reaproveitamento de materiais e buscando minimizar os potenciais impactos ambientais negativos;
- Atender à legislação e adotar normas internas que assegurem o cuidado com o meio ambiente e a qualidade de vida;
- Racionalizar procedimentos operacionais, visando promover a melhoria da



eficiência no consumo energético, dos recursos naturais e dos materiais deles derivados;

- Reduzir ao máximo, se um dia a empresa vier a praticar serviço ou ato que gere efeito direto ao meio ambiente, os impactos ambientais, pautando-se sempre às legislações, normas e convenções internacionais ambientais;
- Buscar ativamente clientes, parceiros e prestadores de serviços que compartilhem e respeitem as regras ambientais estabelecidas pelas legislações, normas e convenções internacionais. Nesse sentido, será priorizada a seleção de colaboradores e parceiros que demonstrem um compromisso sólido com a preservação e proteção do meio ambiente, visando sempre a minimização dos impactos ambientais em todas as etapas das atividades comerciais. Essa abordagem reflete o compromisso contínuo da empresa em promover práticas sustentáveis e contribuir para um futuro mais ecológico e consciente.

2.6.5. Governança para responsabilidade socioambiental

A responsabilidade pela observância e cumprimento desta Política cabe aos membros da Diretoria e a todos os Colaboradores, no limite de suas atribuições. O Departamento Jurídico é responsável por:

- Elaborar e revisar esta Política, sempre que houver mudanças nas práticas da empresa ou em casos de alteração da legislação vigente no tocante aos assuntos socioambientais;
- Alinhar, integrar e estabelecer diretrizes para o desenvolvimento de práticas, programas e projetos socioambientais;
- Avaliar a efetividade das ações implementadas;
- Identificar eventuais deficiências na implementação das ações;
- Garantir a divulgação interna e externa do cumprimento desta Política.
- Informar aos membros da Diretoria sobre eventuais mudanças na Legislação vigente e o impacto disso na empresa.

As Diretorias são responsáveis por:

- Realizar a gestão desta Política;
- Atender aos Órgãos Reguladores nos quesitos das resoluções que dispõem sobre o controle do risco socioambiental.
- Aprovar esta Política, bem como suas futuras alterações e propor aprimoramentos, assegurando a aplicação de suas diretrizes;



2.6.6. Disposições finais

Esta Política representa o compromisso da P4BIT com a promoção da sustentabilidade ambiental e o desenvolvimento social responsável. A implementação desta Política é uma responsabilidade compartilhada por todos os colaboradores e demais integrantes da empresa. A P4BIT também se compromete a fornecer treinamento e capacitação para todos os colaboradores, a fim de garantir a conscientização e adesão a esta política.

A P4BIT reconhece que a responsabilidade socioambiental é uma jornada contínua e está comprometida com esta causa, implementando continuamente ações que contribuam para um futuro mais sustentável e responsável. A empresa se compromete a monitorar continuamente e revisar esta Política, para garantir sua relevância e conformidade com as leis e regulamentos aplicáveis.

Em caso de descumprimento desta Política, serão adotadas as medidas cabíveis conforme o nível e impacto do ato cometido. Caso gestores e colaboradores tomem conhecimento de violação ocorrida, estes deverão comunicar o fato à Diretoria da P4BIT, sob pena de responsabilização. Independentemente do grau de relacionamento com a empresa e da penalidade adotada, aquele que descumprir o estabelecido nesta Política poderá ser responsabilizado civil ou criminalmente sobre as violações comprovadas.

2.7. Política de patrocínio, doações, hospitalidades e brindes

2.7.1. Objetivo

O objetivo desta Política de Patrocínio, Doações, Hospitalidades e Brindes (“Política”) é estabelecer diretrizes, condições e procedimentos para concessão e recebimento de brindes, presentes, doações, hospitalidades, entretenimento, refeições, viagens e outros benefícios monetários e não monetários, por colaboradores, membros da direção, parceiros de negócios e terceiros relacionados à P4BIT.

2.7.2. Abrangência

A presente Política é aplicável a todos os Colaboradores, membros da Diretoria, Parceiros de negócios, Fornecedores e Terceiros que mantenham relação contratual com a P4BIT ou que atuem em seu nome ou benefício, abrangendo ainda todas as atividades desenvolvidas pela empresa.



2.7.3. Definições

- **Brindes:** item institucional oferecido com o logotipo da empresa, a fim promover e divulgar a marca, sendo uma estratégia de comunicação para valorizar e fidelizar a marca. Exemplos: bloco de papel, canetas, calendários, cadernos e mochilas.
- **Presentes:** objetos ou serviços, de uso ou consumo pessoal, que possuam valor comercial e que não se enquadram na definição de Brindes. Também serão considerados "presentes" as hospitalidades de caráter exclusivo de turismo ou de lazer.
- **Hospitalidades:** qualquer tipo de hospitalidade tais como recepções, refeições, hospedagem, despesas de viagem, passagens e/ou deslocamentos (aéreos, marítimos e/ou terrestres), entre outras, que podem ser necessárias para viabilizar negócios.
- **Patrocínios:** bem ou valor negociado que tenha como objetivo o fortalecimento das marcas, produtos e serviços da P4BIT através da associação a projetos de iniciativa de terceiro para promoção de atividades culturais, sociais, esportivas, educacionais e de inovação tecnológica, objetivando obter ganho à imagem institucional, ao relacionamento com seu público e sua reputação.
- **Doações:** concessão de bem (financeiro ou não) pela P4BIT, quando não há, em troca, um benefício acordado (contrapartida).
- **Entretenimento:** atividades ou eventos que tenham como objetivo proporcionar lazer aos seus participantes, como shows, eventos esportivos, festas, concertos, exposições, teatros ou outros tipos de eventos similares.
- **Benefícios Não Monetários:** qualquer tipo de ofertas não-financeiras, como transporte, favores, serviços, garantias e ofertas de emprego.
- **Vantagem Indevida:** oferta, promessa, doação, aceitação ou solicitação de uma vantagem indevida de qualquer valor (financeiro ou não financeiro), direta ou indiretamente, em violação às leis vigentes, como um incentivo ou recompensa para uma pessoa que está agindo ou deixando de agir em relação ao desempenho das suas obrigações.
- **Suborno:** ato de aceitar, prometer, oferecer, receber ou pagar a pessoas físicas e jurídicas, qualquer quantidade de dinheiro, bens materiais e outros benefícios particulares, como diária em hotel, ingressos a shows, cargos, entre outros, a fim de influenciar ou garantir inapropriadamente uma vantagem com relação a um negócio, como contrato, decisão e resultado.
- **Agente Público:** pessoa que exerce função pública, de forma temporária ou permanente, ou que trabalhe para empresa prestadora de serviço contratada



ou conveniada para a execução de atividade típica da Administração Pública; dirigentes de partido político, seus empregados ou outras pessoas que atuem para ou em nome de um partido político ou candidato a cargo político; e pessoas que trabalham em organizações públicas internacionais.

2.7.4. Regras Gerais

A P4BIT mantém um relacionamento cordial e positivo com seus colaboradores e parceiros, no entanto, determina algumas diretrizes para oferecer, conceder e aceitar brindes, presentes, hospitalidades e entretenimentos. Reitera que a prática deve ocorrer de forma ética, transparente e legal e não pode, em hipótese alguma, ser utilizada como contrapartida de nenhuma ação ilícita ou para obtenção de vantagem indevida.

Esta Política estabelece regras para os colaboradores, membros da Direção e parceiros de negócios da P4BIT se comportarem de maneira a evitar situações que possam interferir em decisões ou causar alguma percepção de desconfiança em relação à empresa.

É expressamente proibido que colaboradores, membros da Direção, fornecedores, parceiros de negócios e terceiros que atuam em nome ou em benefício da P4BIT prometam, aceitem, ofereçam e recebam qualquer brinde, presente, entretenimento, hospitalidade nas seguintes situações:

- Com o objetivo de influenciar decisões que afetam a P4BIT ou para obter vantagem indevida para si ou para outrem.
- Quando esteja relacionado a qualquer atividade ilegal.
- Quando o destinatário ou remetente for Agente Público ou Pessoa Exposta Politicamente.
- Com a intenção de criar ou aparentar algum tipo de obrigação ou expectativa futura.

Caso um parceiro de negócios, terceiro ou agente público oferecer ou solicitar brindes, presentes, hospitalidades ou entretenimentos que possam ser interpretados como uma troca por algo ilegal, o colaborador deverá informar imediatamente seu superior imediato e o Departamento Jurídico. Da mesma forma, se um colaborador ou membro da Diretoria oferecer, conceder ou solicitar algo em troca de algo ilegal, a mesma ação deve ser tomada.

Em situações excepcionais, quando se busca iniciar ou estreitar negócios, um parceiro de negócios ou terceiro pode cobrir os custos de brindes, presentes,



hospitalidades ou entretenimentos, desde que seja aprovado pela Diretoria e esteja em conformidade com as condições desta política.

Todos os brindes, presentes, hospitalidades e entretenimentos concedidos devem ser registrados contabilmente de acordo com a legislação em vigor, refletindo a integridade, precisão e exatidão das transações. Operações sigilosas, não registradas ou não informadas são proibidas.

2.7.5. Brindes e presentes

O oferecimento e o recebimento de brindes e presentes podem caracterizar facilmente o favorecimento indevido, suborno, pagamento de facilitação ou corrupção entre as partes envolvidas. Por isso, somente serão considerados regulares os brindes e presentes que seguirem os limites e condições dispostos nesta Política.

Para fins de oferecimento e o recebimento de brindes e presentes, os quais serão fornecidos exclusivamente em eventos da P4BIT, deverão ser observadas as seguintes disposições:

- Devem ser considerados os valores de R\$ 50,00 (cinquenta reais) para brindes de endomarketing e R\$ 100,00 (cem reais) para vale presente de aniversário, ambos por pessoa, como referência de razoabilidade.
- Os brindes concedidos pela P4BIT ou recebidos por colaboradores ou membros da Diretoria devem ser institucionais com a logomarca da Empresa.
- É permitido o oferecimento de brindes promocionais, de valor simbólico, preferencialmente com o nome ou logotipo da P4BIT.
- É permitido conceder brindes em épocas festivas, tais como, Natal, Páscoa, Aniversários, entre outras.
- É proibido conceder presentes/brindes antes de decisões de fechamento de negócio, para pessoa que possua poder de influência nessa decisão.
- Para agentes públicos, é permitido o oferecimento de brindes e eventos com valor unitário de até R\$ 50,00 (cinquenta reais), com distribuição generalizada, ou seja, não deve ser direcionada a um servidor específico, o qual deverá respeitar a periodicidade de 12 (doze) meses, dentro das condições descritas na Resolução Federal nº 3, de 23 de novembro de 2000.

É obrigatório que os colaboradores informem aos membros da Diretoria e ao Departamento Jurídico sobre o recebimento de brindes e presentes que excedam os limites de valores ou de frequência, estabelecidos nesta Política.



No caso dos brindes institucionais, somente haverá a obrigação de informar, caso este exceda os limites de valor ou de frequência. Quando houver dúvida sobre o valor do brinde institucional e a frequência de recebimento, os colaboradores devem buscar informações realizando pesquisas e analisando registros, dentro de suas atribuições e se a dúvida for mantida, também deve informar ao Departamento Jurídico.

2.7.6. Viagens e hospitalidades

As hospitalidades em viagens englobam todos os gastos efetuados com viagens como hospedagem, recepção, passagem, traslado, aluguel de veículos, inscrições e qualquer outro gasto relacionado diretamente com o motivo da viagem. Viagens e deslocamentos são necessários para visitas a fornecedores, parceiros e clientes, participação em feiras, convenções e eventos similares, realização de treinamentos e capacitações, entre outros.

A P4BIT entende esses compromissos profissionais como fundamentais para realização de negócios, aperfeiçoamento e capacitação de seus colaboradores, fortalecer a marca e para estabelecer relacionamento com pessoas e outras instituições.

A P4BIT custeará todos os deslocamentos, hospedagens e inscrições de seus colaboradores para participação em eventos e realização de negócios em que viagens e deslocamentos sejam necessários. Viagens de natureza pessoal, viagens com acompanhantes e familiares e viagens com fins meramente turísticos e de lazer, custeadas ou realizadas em nome da P4BIT, não são permitidas, com exceção daquelas destinadas aos colaboradores (com ou sem acompanhante), que sejam destinatários de premiação ou bonificação por metas de desempenho, conforme as regras previamente definidas e amplamente divulgadas perante todos os colaboradores.

Os colaboradores e membros da Diretoria poderão participar de eventos custeados por parceiros de negócios e terceiros, desde que o evento esteja diretamente ligado a negócios da P4BIT e desde que devidamente aprovado pela Diretoria da Empresa. Para a avaliação e a aprovação, colaborador ou membro da Direção deverá apresentar as informações e justificativas para o recebimento de hospitalidades de viagens, custeadas por terceiros.

Cabe salientar, que as solicitações de viagens e reembolso de despesas com hospitalidades em geral devem respeitar o descrito na Política de Viagens da P4BIT.



2.7.7. Doações e Patrocínio

Todas as doações e patrocínios realizados pela P4BIT têm o propósito de divulgar o nome e a marca da empresa e devem ser efetivados de acordo com as regras dispostas nesta Política e no Manual de Ética, considerando o mais elevado padrão de transparência, integridade e legalidade.

A P4BIT poderá patrocinar projetos com foco nas suas áreas de interesse e atuação e realizar doações a entidades e instituições idôneas e íntegras, motivadas por razões filantrópicas legítimas e em apoio a causas humanitárias, culturais, esportivas e educacionais, bem como ações relacionadas ao bem-estar da comunidade onde a empresa possui operação, sendo que a doação deve ocorrer em conformidade com as regras desta Política.

Para fins desta Política, é vedado à P4BIT e seus respectivos Diretores e Colaboradores:

- Patrocinar projetos, eventos ou materiais de cunho político partidário, religioso, discriminatório ou que infrinjam leis, regulamentos, o Manual de Ética e esta Política;
- Oferecer ou prometer quaisquer tipos de doações ou patrocínios cujo propósito é influenciar, direta ou indiretamente: (i) quaisquer decisões de negócios envolvendo a empresa; (ii) qualquer ação, omissão ou decisão de órgão ou Agente Público; ou (iii) qualquer decisão comercial que seja incompatível com os interesses ou com as políticas internas da empresa.
- Realizar doações ou patrocínios com a finalidade de obter vantagem indevida, ou influenciar a ação de qualquer pessoa, seja agente público, fornecedor, parceiro ou terceiro, independentemente da idoneidade da organização a ser favorecida.
- Realizar doações ou patrocínios para organizações em que colaboradores da empresa ou seus parentes de primeiro grau possuam algum tipo de participação societária e/ou poder de gestão, no intuito de evitar situação que gere potencial conflito de interesses.

Os contratos celebrados com as instituições beneficiadas devem conter a Cláusula Anticorrupção que resguarde a empresa caso a outra parte se envolva em violações das normas da Lei Anticorrupção (Lei nº 12.846) que possam impactar em sua reputação.



2.7.8. Entretenimento

A concessão e o aceite de convites de entretenimento são permitidos somente se estiverem relacionados a situações institucionais como a promoção de serviços e produtos, eventos comerciais e como mera cortesia e prática de boa convivência comercial.

O oferecimento ou recebimento de entretenimento em território nacional e/ou estrangeiro devem estar associados a práticas comerciais de interesse da P4BIT e deverão ser previamente analisados e aprovados pela Diretoria Financeira. Os colaboradores, parceiros de negócios, ou terceiros deverão apresentar à Diretoria, as informações e justificativas para concessão ou recebimento de entretenimentos.

Entretenimentos recebidos ou ofertados para fins meramente turísticos e de lazer só serão permitidos, quando autorizados previamente pela Diretoria da P4BIT.

2.7.9. Responsabilidades

- **Departamento Jurídico:** O Departamento Jurídico desempenha um papel fundamental na elaboração, implementação e monitoramento desta Política, sendo responsável por:
 - Revisar e aprovar esta Política, a fim de garantir que ela esteja em conformidade com as leis e regulamentos aplicáveis e que a empresa siga as melhores práticas éticas de negócios.
 - Fornecer orientação sobre as práticas de negócios éticas e garantir que as práticas da empresa não possam ser interpretadas como suborno ou corrupção.
 - Orientar os colaboradores sobre como gerenciar os riscos associados a patrocínios, doações, hospitalidades e brindes, incluindo a avaliação de terceiros e o monitoramento de conformidade.
 - Aprovar as eventuais alterações e revisões da presente Política.
 - Regulamentar os casos omissos nesta Política.
 - Processar o descumprimento das obrigações e regras estabelecidas nesta Política e deliberar sobre ele, consequentes medidas disciplinares e ações de melhoria de controle, conforme aplicável.
- **Departamento Financeiro:** O Departamento Financeiro desempenha um papel fundamental na gestão desta Política, sendo responsável por:
 - Definir os orçamentos para as atividades de Patrocínio, Doações, Presentes, Viagens, Hospitalidades e Brindes, bem como, estabelecer limites de gastos, a fim de garantir que os recursos sejam utilizados de forma eficiente e em conformidade com a política da empresa, sem



desperdícios.

- Controlar os pagamentos relacionados à Patrocínio, Doações, Presentes, Viagens, Hospitalidades e Brindes e garantir que todos os pagamentos sejam feitos dentro do prazo e em conformidade com as políticas da empresa.
- Identificar e controlar os riscos associados às atividades de Patrocínio, Doações, Presentes, Viagens, Hospitalidades e Brindes, bem como, avaliar o retorno sobre o investimento nestas atividades.
- Lançar de forma suficientemente detalhada e completa nos registros contábeis da P4BIT todas as despesas incorridas relacionadas a Doações, Brindes, Presentes, Viagens e Hospitalidades.
- **Diretorias:** Os membros da Diretoria da P4BIT são responsáveis por garantir a implementação desta Política, bem como, realizar a análise de eventuais casos de exceção às regras estabelecidas neste documento, sendo responsáveis por:
 - Disseminar e aplicar a presente Política em suas respectivas áreas, dar tratamento adequado às concessões ou recebimento de presentes ou hospitalidades fora dos limites estabelecidos nesta Política.
 - Esclarecer eventuais dúvidas dos Colaboradores acerca da concessão, oferta, promessa e/ou recebimento de Brindes, Presentes, Entretenimentos e Hospitalidades.
 - Aprovar a concessão, oferta, promessa e/ou recebimento de Brindes, Presentes, Entretenimentos e Hospitalidades, nos termos previstos na presente Política.
 - Recomendar a destinação de Brindes, Presentes, Entretenimentos ou Hospitalidades recebidos por Colaboradores em desacordo com as diretrizes previstas nesta Política e que não forem passíveis de recusa e/ou devolução.
 - Dar tratamento adequado às concessões ou recebimento de presentes ou hospitalidades fora dos limites estabelecidos nesta Política.
 - Manter registro das comunicações recebidas referentes a interações dos Colaboradores com Agentes Públicos.
 - Reportar ao Departamento Jurídico toda situação relevante de risco ou descumprimento desta Política, recomendando medidas disciplinares e eventuais melhorias de controle.

Por fim, é dever de todos os Colaboradores, membros da Direção e terceiros seguir os princípios e regras contidos no Manual de Ética e Conduta Empresarial, assim como nesta Política.



2.7.10. Canal de denúncia

O canal de denúncia é gerenciado pela P4BIT, responsável pelo processamento das denúncias recebidas e encaminhamento para apuração do Departamento Jurídico. Toda e qualquer denúncia poderá ser feita anonimamente, sendo a identidade do denunciante protegida durante todo o processo de apuração se ele assim o desejar.

As denúncias podem ser feitas por meio do nosso Canal de Denúncia, através do e-mail: compliance@p4bit.com.

2.7.11. Disposições finais

A presente Política passa a vigorar para todos os colaboradores, membros da Diretoria, terceiros, fornecedores e parceiros de negócios da P4BIT, após a aprovação da Diretoria e do Departamento Jurídico.

A P4BIT pode, por sua mera liberalidade ou em razão de alterações legislativas, a qualquer momento, revisar os termos do presente Estatuto, sendo que em caso de alteração será submetida a nova aprovação. Quaisquer omissões, interpretações e exceções deverão ser levadas à análise do Departamento Jurídico.

Atualizado em 15 de janeiro de 2026.

