



POLÍTICA

DE PRIVACIDADE, PROTEÇÃO DE DADOS PESSOAIS, SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

Abril 2026



ÍNDICE

HISTÓRICO DE REVISÃO	3
I. INTRODUÇÃO	4
II. ESCOPO E ABRANGÊNCIA	4
III. OBJETIVOS E DIRETRIZES GERAIS	5
IV. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS	6
(i) DEFINIÇÕES.....	6
(ii) CONSENTIMENTOS GERAIS PELOS TITULARES.....	7
(iii) DE QUE FORMA A DAHLIA CAPITAL COLETA SEUS DADOS PESSOAIS?.....	8
(iv) QUAIS DADOS PESSOAIS SÃO TRATADOS PELA DAHLIA CAPITAL?	8
(v) COMPARTILHAMENTO DE DADOS COM TERCEIROS.....	10
(vi) ARMAZENAGEM E TÉRMINO DO TRATAMENTO DE DADOS	11
(vii) INVENTÁRIO DE DADOS PESSOAIS	11
(viii) DIREITOS DOS TITULARES	11
(ix) COMO O TITULAR PODE EXERCER SEUS DIREITOS?	12
(x) DADOS PESSOAIS SENSÍVEIS E DADOS PESSOAIS NÃO SOLICITADOS	13
(xi) <i>POLÍTICA DE COOKIES</i>	13
(xii) RECRUTAMENTO	15
(xiii) SITES DE TERCEIROS	15
(xiv) COMO ENTRAR EM CONTATO COM A DAHLIA CAPITAL	15
V. SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA	16
(i) CHEFE DE SEGURANÇA DA INFORMAÇÃO.....	16
(ii) SUBCOMITÊ DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO	16
(iii) INFORMAÇÕES SIGILOSAS	17
(iv) EQUIPAMENTOS CORPORATIVOS.....	18
(v) SITES E DOWNLOADS	18
(vi) ACESSOS FÍSICOS E DIGITAIS.....	19
(vii) PROTEÇÃO DE DADOS PESSOAIS.....	20
(viii) IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS	21
(ix) AÇÕES DE PREVENÇÃO E PROTEÇÃO	22
(x) MONITORAMENTO DE TERCEIROS	23
(xi) TREINAMENTO DE COLABORADORES.....	25
(xii) TESTES PERIÓDICOS DE SEGURANÇA DA INFORMAÇÃO	25
VI. POLÍTICA DE BYOD	26
VI. POLÍTICA DE SENHAS	28
VI. VIGÊNCIA E ATUALIZAÇÃO	29
ANEXO I	30
ANEXO II	31
(i) PAPÉIS E RESPONSABILIDADE	31
(ii) ESTÁGIOS DO PRI.....	32
(iii) INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS.....	32

HISTÓRICO DE REVISÃO

VERSÃO	DATA	DESCRIÇÃO	REVISÃO	APROVAÇÃO FINAL
1	Janeiro/2018	Primeira Emissão	Compliance DAHLIA	Paulo Lowndes Dale Diretor de Riscos, Compliance, PLDFT e DPO
2	Abril/2020	Revisão Completa	Compliance DAHLIA	Paulo Lowndes Dale Diretor de Riscos, Compliance, PLDFT e DPO
3	Agosto/2021	Revisão para incluir aspectos de privacidade/proteção de Dados Pessoais e reforçar itens de Segurança da Informação	Compliance DAHLIA	Paulo Lowndes Dale Diretor de Riscos, Compliance, PLDFT e DPO
4	Setembro/2022	Revisão anual de rotina e inclusão de pontos trazidos pelo novo Código de ART ANBIMA (em audiência pública)	Compliance DAHLIA	Paulo Lowndes Dale Diretor de Riscos, Compliance, PLDFT e DPO
5	Outubro/2023	Revisão anual de rotina, inclusão de novas boas práticas trazidas pela ANPD e endereçamento de recomendações dadas no contexto de PenTest realizado junto à KPMG	Compliance DAHLIA	Erica Yam Diretora de Riscos, Compliance, PLDFT e DPO
6	Dezembro/2024	Revisão anual de rotina e inclusão de novas disposições por conta da Resolução CD/ANPD nº 15, de 24 de abril de 2024 (sobre incidente de segurança) e Resolução CD/ANPD nº 18/2024, de 16 de julho de 2024 (sobre encarregado)	Compliance DAHLIA	Erica Yam Diretora de Riscos, Compliance, PLDFT e DPO
7	Abril/2026	Revisão anual de rotina e inclusão de novas disposições alinhadas à 4ª edição do Guia ANBIMA de Cibersegurança e à Resolução CMN nº 5.274/2025 (a qual altera regras de segurança cibernética para instituições financeiras reguladas pelo Banco Central, utilizada apenas como referência).	Compliance DAHLIA	Erica Yam Diretora de Riscos, Compliance, PLDFT e DPO

I. INTRODUÇÃO

No âmbito de suas atividades, a Dahlia Capital Gestão de Recursos Ltda., inscrita no CNPJ nº 09.551.766/0001-39, com sede na Rua Joaquim Floriano, 940, Conj 11 e 12, no Bairro Itaim Bibi, na Cidade de São Paulo, no Estado de São Paulo, CEP: 04534-004 ("**Dahlia Capital**" ou "**Gestora**") adota mecanismos técnicos e administrativos que visam assegurar a segurança, a confidencialidade, a integridade, a privacidade e a disponibilidade de informações e dados tratados pela Gestora e seus equipamentos e sistemas de informação.

A presente Política de Privacidade, Proteção de Dados Pessoais, Segurança da Informação e Cibersegurança ("**Política**") documenta as práticas institucionais adotadas pela Dahlia Capital relativas à privacidade, proteção de dados pessoais, segurança da informação e cibersegurança, refletindo, assim, os procedimentos relacionados a serem observados por todos os seus Colaboradores no exercício de suas atividades. Esta Política adota abordagem baseada em risco e proporcionalidade, considerando o porte, a complexidade e o modelo de negócios da Gestora, em linha com as melhores práticas de mercado e orientações da ANBIMA. Adicionalmente, esta Política poderá observar, como referência de boas práticas, normativos aplicáveis ao sistema financeiro nacional, incluindo disposições do Conselho Monetário Nacional sobre segurança cibernética.

Esta Política é uma declaração formal da Dahlia Capital acerca de seu compromisso com a proteção de informações e dados de sua propriedade e/ou sob sua guarda e com a transparência acerca do tratamento de dados pessoais realizado pela Dahlia Capital junto a seus respectivos titulares.

Os termos em letra maiúscula utilizados ao longo desta Política terão os significados aqui especificados ou definidos na legislação aplicável.

II. ESCOPO E ABRANGÊNCIA

Esta Política e as regras nela descritas aplicam-se a todos os sócios, administradores, diretores, empregados, estagiários e prestadores de serviços ("**Colaboradores**") da Dahlia Capital que acessem ou sejam usuários de qualquer ambiente, recurso, equipamento e/ou o sistema de informação da Gestora, seja de forma física, remota ou através de terceiros.

As disposições relativas ao tratamento de dados pessoais pela Dahlia Capital são direcionadas a todos que sejam pessoas naturais, titulares de dados pessoais tratados pela Dahlia Capital, incluindo (i) aqueles que sejam investidores dos fundos de investimento cujas carteiras são geridas pela Dahlia Capital ("**Investidor**" e "**Fundos**") e (ii) os usuários do Site Dahlia ("**Usuário**").

A Dahlia Capital não realiza a distribuição de cotas de fundos de investimento sob sua gestão e não possui qualquer responsabilidade pelo relacionamento direto com o Investidor, função que é desempenhada pelos distribuidores contratados diretamente pelos Fundos. Nesse sentido, a presente Política é também direcionada aos Investidores *exclusivamente* para fins de dar a necessária transparência exigida pela legislação aplicável – notadamente a Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018 ou “LGPD”) – acerca do tratamento de dados pessoais de tais Investidores pela Dahlia Capital, nos casos em que, extraordinariamente, a Dahlia Capital venha a ter acesso a tais Dados Pessoais, tendo em vista procedimentos operacionais impostos pelos distribuidores dos Fundos, nos termos da regulamentação aplicável as suas atividades.

O Usuário, Investidor e qualquer terceiro titular de dados pessoais tratados pela Dahlia Capital devem ler atenta e integralmente o presente documento antes de utilizar o Site Dahlia Capital ou estabelecer qualquer relacionamento empregatício, comercial e/ou contratual com a Dahlia Capital. O acesso e navegação a qualquer área do Site Dahlia, o estabelecimento de relação empregatícia, comercial ou contratual ou o fornecimento espontâneo de dado pessoal sob qualquer meio à Dahlia Capital será interpretado como aceite formal e integral da presente Política. Caso o investidor, usuário ou terceiro titular não concorde com qualquer disposição desta Política, recomendamos que contate imediatamente seu distribuidor ou a Dahlia Capital (nos meios indicados no item IV (xiii)), conforme o caso.

III. OBJETIVOS E DIRETRIZES GERAIS

Esta Política e todas as práticas e procedimentos aqui descritos têm como objetivo proteger dados e informações da Dahlia Capital, de Investidores, Colaboradores, usuários do Site Dahlia, parceiros comerciais e/ou de quaisquer terceiros que sejam tratados pela Dahlia Capital ou estejam sob sua guarda, garantindo a respectiva privacidade, segurança, integridade, confidencialidade, disponibilidade e auditabilidade nos termos da legislação aplicável.

Adicionalmente, a presente Política visa fornecer aos Investidores, Usuários titulares de Dados Pessoais tratados pela Dahlia Capital informações claras e precisas acerca das práticas e regras relacionadas ao referido tratamento nas diferentes atividades desempenhadas pela Dahlia Capital e no âmbito do Site Dahlia.

A Dahlia Capital reconhece a importância da proteção de dados pessoais e disponibiliza esta Política publicamente em seu website com todas as informações importantes acerca da coleta, compartilhamento, armazenagem e tratamento de dados pessoais realizados pela Dahlia Capital, bem como as formas de exercício dos direitos conferidos aos respectivos

Titulares nos termos da legislação aplicável, as medidas de segurança adotadas para prevenir e remediar incidentes e os dados de contato da DPO da Dahlia Capital.

A Dahlia Capital adota como regra geral a não divulgação de nenhuma informação ou dado, incluindo dados pessoais, em qualquer hipótese, a pessoas, dentro ou fora da Dahlia Capital, que não necessitem de, ou não devam ter, acesso a tais informações ou dados para desempenho de suas atividades e funções profissionais.

Qualquer informação sobre a Dahlia Capital, ou de qualquer natureza relativa às atividades da Dahlia Capital, de seus sócios, Colaboradores, Investidores, parceiros comerciais e/ou terceiros com quem a Dahlia Capital se relaciona, obtida em decorrência do desempenho das atividades e funções de qualquer Colaborador, só poderá ser fornecida a terceiro nas hipóteses expressamente autorizadas pela presente Política ou sob autorização expressa da Diretora de Riscos e Compliance/DPO nomeada pela Dahlia Capital, nos termos da legislação aplicável.

Todo e qualquer Colaborador da Dahlia Capital assume o compromisso e a responsabilidade de proteger a privacidade, a segurança, a confidencialidade, a integridade e a disponibilidade das informações e dados tratados e dos equipamentos e sistemas da Dahlia Capital no exercício de suas atividades e funções.

IV. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Este capítulo tem como objetivo descrever as práticas e procedimentos relacionados ao tratamento de dados pessoais realizado pela Dahlia Capital no contexto da prestação dos serviços de administração de carteira aos Fundos ("**Serviços**") e na gestão de seu website (www.dahliacapital.com.br e demais páginas deste domínio) ("**Site Dahlia**").

A Dahlia Capital realiza o tratamento de dados pessoais para viabilizar a prestação dos serviços e o funcionamento do Site Dahlia, incluindo, sem limitação, dados que pertençam a Investidores, usuários do Site Dahlia e indivíduos que celebrem, diretamente ou na qualidade de representantes de pessoas jurídicas, contratos de qualquer natureza com a Dahlia Capital. Ao fazê-lo, a Dahlia Capital e todos os seus Colaboradores devem sujeitar-se às disposições da LGPD, normas e orientações da Autoridade Nacional de Proteção de Dados ("**ANPD**"), regras e boas práticas de órgãos de autorregulação (i.e. ANBIMA) e pelas disposições da presente Política.

(i) Definições

- Agentes de Tratamento – o Controlador ou o Operador.
- Banco de Dados – conjunto estruturado de Dados Pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

- Browser – software criado para possibilitar navegação na internet.
- Cookies – arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas, como, por exemplo, o melhor funcionamento do website.
- Consentimento – manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus Dados Pessoais para uma finalidade determinada.
- Controlador – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao Tratamento de Dados Pessoais.
- Dado Pessoal – informação relacionada a pessoa natural identificada ou identificável.
- Dado Pessoal Sensível – Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- DPO – encarregado indicado pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os Titulares dos Dados Pessoais e a ANPD, nos termos da LGPD e demais regulações aplicáveis.
- Operador – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de Dados Pessoais em nome do Controlador.
- Titular – pessoa natural a quem se referem os Dados Pessoais que são objeto de tratamento.
- Tratamento – 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.

(ii) Consentimentos gerais pelos Titulares

Ao ler esta Política, a Dahlia Capital quer que você, Usuário, Investidor e/ou terceiro Titular, saiba com clareza e precisão com o que está concordando. Por isso, ao aceitar a presente Política, você declara que sabe e concorda:

- a. que é o Titular ou que possui todas as autorizações legais relacionadas aos Dados Pessoais de terceiros compartilhados com a Dahlia Capital em razão dos Serviços, tendo tais dados sido obtidos por meios e fontes legais e legítimas;
- b. que é responsável pela veracidade e integridade de referidos Dados Pessoais, sujeitando-se às medidas legais cabíveis pela violação dessas declarações; e
- c. que a Dahlia Capital e os Agentes de Tratamento poderão realizar o Tratamento de seus Dados Pessoais conforme descrito nesta Política.

(iii) De que forma a Dahlia Capital coleta seus Dados Pessoais?

A coleta de Dados Pessoais pela Dahlia Capital é limitada ao exigido pela legislação aplicável ou ao mínimo necessário para a condução dos Serviços e atividades da Dahlia Capital e gestão do Site Dahlia. A Dahlia Capital pode coletar seus Dados Pessoais das seguintes formas:

- a. Investidores:** Em razão de exigências legais ou regulatórias ou de obrigações contratuais, a Dahlia Capital poderá realizar o tratamento de Dados Pessoais de identificação de Investidores, nos casos em que extraordinariamente, a Dahlia Capital venha a ter acesso a tais Dados Pessoais;
- b. Usuários:** fornecimento direto pelos Usuários à Dahlia Capital na utilização dos recursos de comunicação e inscrição para recebimento de informativos, cartas da gestão e *newsletter* e/ou pelo registro de *cookies* durante a navegação no Site Dahlia;
- c. Outros:** fornecimento direto pelo Titular à Dahlia Capital, por qualquer meio (ex. e-mail, cartão de contato, reuniões, ligação telefônica, etc) no contexto de uma solicitação ou situação específica (ex. reuniões comerciais, recrutamento, pedido de informações, entre outros).

(iv) Quais Dados Pessoais são tratados pela Dahlia Capital?

A **Tabela 1** abaixo detalha quais Dados Pessoais podem ser tratados pela Dahlia Capital, suas finalidades e os fundamentos legais que legitimam seu tratamento, nos termos da LGPD:

Propósitos/Finalidades	Fundamento legal	Dados Pessoais
Prestação dos Serviços e atendimento de exigências legais e regulatórias e/ou obrigações contratuais Em razão de exigências legais ou regulatórias ou de obrigações contratuais aplicáveis ao Controlador (ex. distribuidores e administrador fiduciário dos Fundos), a Dahlia Capital poderá realizar o tratamento de Dados Pessoais de identificação de Investidores , nos casos em que, extraordinariamente, a Dahlia Capital venha a ter acesso a tais Dados Pessoais.	A depender da finalidade específica: Cumprimento de obrigação legal ou regulatória pelo Controlador; Execução de contrato pelo Controlador	Os Dados Pessoais podem incluir, entre outros, dados de identificação, cadastro e contato (como nome completo, nacionalidade, filiação, estado civil, profissão, endereço, e-mail, número de telefone, RG/RNE e CPF), dados bancários e financeiros e informações familiares.
Canal de Comunicação com o Titular Em resposta e/ou atendimento de solicitações recebidas por e-mail, correspondência física, redes sociais, canal de comunicação do Site Dahlia, serviço de mensageria (ex. Whatsapp) ou ligação telefônica, a Dahlia Capital poderá realizar o tratamento de Dados Pessoais de Investidores e/ou Usuários cadastrados no Site Dahlia para responder a solicitações e/ou enviar cartas da gestão e materiais informativos dos Fundos por e-mail.	Consentimento do Titular	Os Dados Pessoais podem incluir dados de identificação e contato (ex. nome, e-mail, telefone).

Propósitos/Finalidades	Fundamento legal	Dados Pessoais
<p>Processamento de Dados Pessoais de Usuários do Site Dahlia</p> <p>A Dahlia Capital poderá processar Dados Pessoais e de acesso de Usuários de forma automatizada e codificada no âmbito da navegação no Site Dahlia por meio de cookies, a fim de possibilitar o funcionamento do site, organizar e estruturar tais dados para gerar informações e estatísticas gerais não individualizadas ("Dados Não Individualizados") para melhor desenvolvimento dos Serviços, bem como registro de aceitação de Avisos Legais.</p>	<p>A depender da finalidade específica:</p> <p>Consentimento do Titular</p> <p>Legítimo Interesse (no caso de cookies essenciais para o funcionamento)</p> <p>Cumprimento de obrigação legal ou regulatória pelo Controlador (no caso do registro de aceitação de Avisos Legais)</p>	<p>Os Dados Pessoais podem incluir, dentre outros, o navegador de acesso do Titular; endereço do protocolo de Internet (IP); data e hora do acesso; e as eventuais ações do Titular no Site Dahlia (ex. aceitação de Aviso Legal).</p>
<p>Relacionamento com parceiros comerciais, prestadores de serviços e companhias investidas</p> <p>Para fins de estabelecimento e manutenção de relacionamento com parceiros comerciais, prestadores de serviços dos Fundos ou da Dahlia Capital (ex. distribuidores, contabilidade) e/ou companhias investidas pelos Fundos os quais sejam necessários para a execução dos Serviços, a Dahlia Capital poderá realizar o tratamento de Dados Pessoais de indivíduos representantes ou membros dos órgãos de administração de referidos parceiros, prestadores e/ou companhias no contexto da execução dos Serviços ou atividades correlatas com fim comercial, pesquisa, votação em assembleias, ou execução de contrato ou diligências prévias com o parceiro e/ou prestador de serviço, organização de ou participação em eventos virtuais/presenciais ou de atendimento a requerimentos legais ou regulatórios (ex. gestão do programa de Compliance e regulamentação de PLD-FTP).</p>	<p>A depender da finalidade específica:</p> <p>Consentimento do Titular;</p> <p>Execução de contrato ou diligências prévias;</p> <p>Cumprimento de obrigação legal ou regulatória</p>	<p>Os Dados Pessoais podem incluir dados de identificação e contato (ex. nome, e-mail, telefone, empresa, cargo).</p>
<p>Recrutamento</p> <p>Para fins de preenchimento de posições em aberto na Dahlia Capital e potencial contratação de novos Colaboradores, a Dahlia Capital poderá realizar o tratamento de Dados Pessoais de candidatos ou potenciais candidatos às vagas recebidos por qualquer meio, diretamente do Titular ou mediante indicação de terceiro, com o propósito de avaliar, por si ou através de terceiros, se o candidato possui os requisitos necessários para a vaga disponível, criação de inventário de currículos e/ou agendamento de entrevistas.</p>	<p>Consentimento do Titular</p>	<p>Os Dados Pessoais podem incluir dados de identificação e contato (ex. nome, e-mail, telefone) e histórico profissional e acadêmico.</p>

(v) **Compartilhamento de dados com terceiros**

Conforme indicado acima, em alguns casos, a Dahlia Capital conta com Agentes de Tratamento para a realização do tratamento dos Dados Pessoais.

Os Agentes de Tratamento que possam ter acesso a Dados Pessoais tratados pela Dahlia Capital prestam serviços como: (i) administração fiduciária de fundos de investimento; (ii) distribuição de cotas de fundos de investimento; (iii) outros serviços financeiros relacionados à indústria de fundos de investimento (ex. gestão de carteira de fundos investidores dos Fundos); (iv) serviços de infraestrutura tecnológica e bases de dados em nuvem; (v) serviços de marketing e branding, (vi) serviços de assessoria jurídica, regulatória, financeira ou contábil; (vii) provedor de sistema de gestão de Compliance, (viii) serviços de auditoria, entre outros. A Dahlia Capital realiza avaliação prévia de risco (*risk-based due diligence*) dos terceiros com acesso a dados pessoais e revisões periódicas proporcionais à criticidade do serviço, nos termos de sua Política de Contratação de Terceiros.

A Dahlia Capital só compartilha Dados Pessoais com Agentes de Tratamento dentro dos propósitos e finalidades indicados na **Tabela 1**. Porém, excepcionalmente, Dados Pessoais somente poderão ser compartilhados com terceiros nas hipóteses descritas na **Tabela 2** abaixo:

Tabela 2 – Compartilhamento de Dados Pessoais	
Ordem judicial ou requisição de autoridade competente	A Dahlia Capital poderá compartilhar os dados coletados do Titular quando solicitados (i) por meio de ordem judicial ou (ii) por requisição de autoridade competente nos termos da legislação aplicável.
Novas Funcionalidades, Negócios ou Parcerias	A Dahlia Capital poderá compartilhar Dados Pessoais e Dados Não Individualizados com potenciais parceiros comerciais ou prestadores de serviços com o objetivo de implementar novas funcionalidades no Site Dahlia ou melhorias nos Serviços, ou, ainda, expandir os negócios e serviços oferecidos pela Dahlia Capital. Entretanto, nas hipóteses em que o Dado Pessoal tenha sido coletado com base no Consentimento, o Titular sempre será notificado para que autorize o compartilhamento ou a utilização do dado para a nova finalidade. Além disso, a Dahlia Capital não poderá compartilhar ou utilizar para novas finalidades Dados Pessoais tratados na qualidade de Operador em nome de Controlador terceiro. Caso o Titular opte por não autorizar o uso do dado ou seu compartilhamento, seus Dados Pessoais não serão utilizados ou transmitidos a terceiros.
Análise de dados estatísticos e de mercado	Os Dados Não Individualizados ou quaisquer dados anonimizados, ou seja, sem a identificação dos Titulares, poderão ser utilizados pela Dahlia Capital para construção de planilhas estatísticas ou análises de mercado, que poderão ser compartilhadas com terceiros.
Suspeita de conduta potencialmente ilegal ou fraudulenta	A Dahlia Capital poderá compartilhar Dados Pessoais com terceiros e autoridades quando suspeitar de prática de atos ilícitos envolvendo Titulares e relacionado às atividades da Dahlia Capital, incluindo no contexto de processos administrativos, judiciais ou arbitrais.

Exceto nos casos permitidos pela legislação aplicável, os Dados Pessoais de Titulares, Investidores ou Usuários não serão objeto de cessão a terceiros pela Dahlia Capital sem a prévia autorização dos Titulares. Em qualquer caso, o compartilhamento de Dados Pessoais observará todas as leis e regras aplicáveis, buscando sempre garantir a privacidade, segurança e integridade dos dados, observados os padrões técnicos disponíveis e boas práticas adotadas no mercado.

(vi) Armazenagem e término do tratamento de dados

Os Dados Pessoais coletados pela Dahlia Capital são armazenados e utilizados pelo período necessário para atingir as finalidades elencadas na **Tabela 1**, considerando os direitos de seus Titulares, as responsabilidades dos Agentes de Tratamento e as disposições legais ou regulatórias aplicáveis.

Após o término do tratamento, a Dahlia Capital poderá manter sob sua guarda e/ou *back up* todos os dados e documentos necessários para o exercício regular de seus direitos em eventuais processos administrativos, judiciais ou arbitrais, considerando o prazo prescricional máximo estabelecido em lei.

Uma vez expirados os períodos de armazenamento dos Dados Pessoais, eles serão removidos da base de dados ou anonimizados, salvo nos casos em que houver a possibilidade ou a necessidade de armazenamento em virtude de disposição legal ou regulatória.

(vii) Inventário de Dados Pessoais

A Dahlia Capital mantém Inventário de Dados Pessoais nos termos da LGPD visando o registro das operações de tratamento realizadas no âmbito de sua atividade. Desta forma, os Controladores e Operadores envolvidos nos tratamentos de Dados Pessoais realizados pela Dahlia Capital também são mapeados e identificados por meio do referido documento.

(viii) Direitos dos Titulares

O Titular de Dados Pessoais tratados pela Dahlia Capital possui os seguintes direitos, conferidos pela LGPD:

Tabela 3 – Direitos dos Titulares	
Direitos	Descrição
Confirmação	O Titular pode requerer a confirmação de quais de seus Dados Pessoais são objeto de coleta e tratamento pela Dahlia Capital.
Acesso	O Titular pode requisitar, a qualquer momento, uma cópia dos Dados Pessoais sob custódia da Dahlia Capital e de sua titularidade.

Tabela 3 – Direitos dos Titulares	
Direitos	Descrição
Correção	O Titular pode, a qualquer momento, solicitar a correção de seus Dados Pessoais. Para efetivar a correção, a Dahlia Capital checará a veracidade e titularidade dos Dados Pessoais fornecidos.
Anonimização, bloqueio ou eliminação	Nos limites permitidos pela legislação, o Titular pode requerer a suspensão temporária de qualquer operação de tratamento de seus Dados Pessoais e solicitar sua exclusão da base de dados da Dahlia Capital quando entender que são desnecessários ou excessivos.
Portabilidade	O Titular possui o direito de solicitar a transferência de seus Dados Pessoais a outro prestador de serviços*, salvo em relação aos Dados Pessoais já anonimizados pela Dahlia Capital. <i>*No tocante a dados de Investidores, é importante frisar que a Dahlia Capital só trata Dados Pessoais em casos extraordinários e na qualidade de Operador, tendo em vista procedimentos operacionais impostos pelos distribuidores dos Fundos, sendo o tratamento realizado dentro das finalidades e sob instrução do distribuidor, que é o prestador de serviços responsável pelo relacionamento direto com o Investidor e o Controlador dos respectivos Dados Pessoais.</i>
Exclusão	O Usuário poderá requerer a exclusão de seus Dados Pessoais tratados com base no Consentimento (vide Tabela 1 desta Política). É importante destacar que, nos termos da LGPD, não existe um direito de eliminação de dados tratados com fundamento em bases legais distintas do Consentimento, a menos que os dados sejam desnecessários, excessivos ou tratados em desconformidade com o previsto na lei.
Compartilhamento	O Titular possui o direito de ser informado acerca de todas as entidades com as quais seus Dados Pessoais são compartilhados.
Não Consentimento	O Titular pode não consentir com o tratamento de seus Dados Pessoais pela Dahlia Capital, ressalvado os casos em que não é necessário o Consentimento para seu tratamento (vide Tabela 1 desta Política). No caso de retirada do Consentimento, a Dahlia Capital poderá ficar impossibilitada de realizar atividades relacionadas aos Serviços, sendo que, nesta hipótese, tal fato não resultará qualquer infração pela Dahlia Capital.
Revogação do Consentimento	O Titular poderá revogar seu Consentimento acerca do tratamento de seus Dados Pessoais pela Dahlia Capital, ressalvado os casos em que não é necessário o Consentimento para seu tratamento (vide Tabela 1 desta Política), sendo que o tratamento realizado previamente à solicitação continuará válido. A revogação dos Consentimentos expressos nesta Política pode resultar na impossibilidade e inviabilização do uso do Site Dahlia e execução dos Serviços relativamente ao Titular (incluindo a operacionalização de aplicações de recursos nos Fundos por parte deste).

(ix) Como o Titular pode exercer seus direitos?

Os Titulares, Usuários e Investidores poderão exercer os direitos mencionados na **Tabela 3** mediante solicitação expressa à Dahlia Capital, a qualquer tempo e por qualquer razão, dentro dos propósitos e condições estabelecidos na legislação aplicável. Para tanto, é necessário entrar em contato com a Dahlia Capital* através de [Canal LGPD](#) disponibilizado no Site Dahlia ou das informações de contato do DPO fornecidas nesta Política. ***No tocante a Investidores dos Fundos, importante ler o aviso em destaque incluído no item II (Escopo e Abrangência) desta Política e entrar em contato com o seu respectivo distribuidor.**

Para garantir que o Titular que pretende exercer seus direitos é, de fato, o Titular dos Dados Pessoais objeto da requisição, a Dahlia Capital poderá solicitar documentos ou outras informações que possam auxiliar em sua correta identificação, a fim de resguardar direitos próprios e de terceiros. Isto somente será feito, porém, se for absolutamente necessário, e o requerente receberá todas as informações relacionadas.

A Dahlia Capital terá até 15 (quinze) dias úteis para cumprir com a solicitação do Titular e, mediante apresentação de justificativa, a depender do volume e complexidade da solicitação, este prazo poderá ser estendido por mais 30 (trinta) dias úteis ou por prazo superior a ser acordado com o Titular.

A Dahlia Capital alerta que a exclusão de Dados Pessoais ou a revogação dos Consentimentos expressos nesta Política pode resultar na impossibilidade e inviabilização do uso do Site Dahlia e da execução dos Serviços relativamente ao Titular.

(x) Dados Pessoais sensíveis e Dados Pessoais não solicitados

A Dahlia Capital solicita que nenhum Dado Pessoal Sensível seja diretamente fornecido à Dahlia Capital a não ser que expressamente solicitado. Eventualmente, se forem necessários, Dados Pessoais considerados sensíveis somente serão disponibilizados pelo Titular mediante seu Consentimento específico e destacado. Em qualquer caso, o tratamento de Dados Pessoais sensíveis somente ocorrerá para atender a finalidades específicas.

Ao aceitar a presente Política, o Titular que enviar Dados Pessoais Sensíveis ou Dados Pessoais não solicitados à Dahlia Capital e seus Colaboradores está ciente e concorda que estará automaticamente autorizando a Dahlia Capital a realizar o tratamento de tais dados com a única e exclusiva finalidade de excluí-los.

(xi) Política de Cookies

Conforme elencado na **Tabela 1**, responsável por detalhar quais Dados Pessoais podem ser tratados pela Dahlia Capital, suas finalidades e os fundamentos legais que legitimam seu tratamento, nos termos da LGPD, ao acessar o Site Dahlia, *cookies* poderão ser gravados nos dispositivos de Usuários. Conforme o Capítulo de Definições, *cookies* são arquivos instalados no dispositivo de um usuário que permitem a coleta de determinadas informações, inclusive de dados pessoais em algumas situações, visando ao atendimento de finalidades diversas, como, por exemplo, o melhor funcionamento do website. Os *cookies* não permitem que arquivos ou informações sejam extraídos do disco rígido do Usuário, não sendo possível, portanto, que, por meio deles, se tenha acesso a informações pessoais que não tenham partido do Usuário ou da forma como ele utiliza os recursos do Site Dahlia.

Finalidade: Eles servem, basicamente, para que seja possível identificar dispositivos, atividades e preferências de Usuários a fim de possibilitar o funcionamento do site e melhorar a experiência do usuário.

Hipótese de tratamento:

- Consentimento do Titular (no caso de cookies de marketing, funcionais ou analíticos)
- Legítimo Interesse (no caso de cookies essenciais para o funcionamento)
- Cumprimento de obrigação legal ou regulatória pelo Controlador (no caso do registro de aceitação de Avisos Legais)

Período de retenção: A maioria dos *cookies* utilizados no Site Dahlia serão apagados automaticamente ao encerrar a sessão do navegador, excetuados os *cookies* que contêm informações sobre o endereço de IP, que permanecerão no seu computador, possibilitando identificação na próxima visita ao Site Dahlia.

Compartilhamento com terceiros: Todas as informações referentes a compartilhamentos de dados pessoais realizados pela Dahlia Capital estão descritas no Capítulo "Compartilhamento de dados com terceiros"

Cookies de terceiros: Alguns de nossos parceiros podem configurar *cookies* nos dispositivos de Usuários que acessam e navegam nos links relativos a tais parceiros a partir do Site Dahlia. Estes *cookies*, em geral, visam possibilitar que nossos parceiros possam oferecer seu conteúdo e seus serviços ao Usuário que acessa nosso site de forma personalizada, por meio da obtenção de dados de navegação extraídos a partir de sua interação com links acessados a partir do Site Dahlia. As entidades encarregadas da coleta de tais *cookies* poderão ceder as informações obtidas a terceiros sem qualquer controle ou ingerência por parte da Dahlia Capital. Uma vez que o Usuário acesse e navegue em tais links de terceiros, não há qualquer responsabilidade por parte da Dahlia Capital e os termos de uso daquele link/website específico não estão abrangidos pela presente Política.

Os Usuários poderão impedir a instalação de *cookies* a qualquer momento por meio de alteração nas configurações de seus Browsers, a partir dos seguintes links:

Browser	Gestão de Cookies
Internet Explorer	https://support.microsoft.com/pt-br/help/17442/windows-internet-explorer-delete-manage-cookies
Safari	https://support.apple.com/pt-br/guide/safari/sfri11471/mac
Google Chrome	https://support.google.com/chrome/answer/95647?hl=pt-BR&hlrm=pt
Opera	https://www.opera.com/help/tutorials/security/privacy/

(xii) Recrutamento

Ao enviar currículo profissional ou documento de natureza similar à Dahlia Capital, o Titular – ou terceiro que o indicar – estará automaticamente autorizando o tratamento dos Dados Pessoais presentes no referido documento pela Dahlia Capital – incluindo sua transferência a terceiros – com a finalidade de avaliar se o respectivo candidato possui os requisitos necessários para a posição disponível no momento. Em caso de não contratação, os currículos permanecerão na Base de Dados da Dahlia Capital por **até 3 anos**, podendo ser reanalisados para futuras oportunidades. Findo o prazo, os currículos serão excluídos permanentemente. O Titular poderá retirar o seu consentimento a qualquer momento. Nesse caso, a Dahlia Capital não poderá considerá-lo para as oportunidades de emprego.

(xiii) Sites de terceiros

O Site Dahlia poderá ter em seu conteúdo links de outros sites, o que não significa que esses sites sejam de propriedade ou operados pela Dahlia Capital. Ao clicar nestes anúncios ou links, o Usuário ou o Investidor será direcionado para o site destes terceiros e, portanto, a partir deste ponto deverá observar as políticas, termos de uso e privacidade do site em questão.

(xiv) Como entrar em contato com a Dahlia Capital

Para esclarecimento de quaisquer dúvidas sobre esta Política ou sobre Dados Pessoais que são tratados pela Dahlia Capital, o Titular poderá entrar em contato com o nosso DPO, por algum dos canais mencionados abaixo:

- **Canal LGPD - <https://dahlia.compliasset.com/lgpd-dahlia>**
- **Contato ou correspondência direta para o Encarregado/DPO da Dahlia Capital:**
Erica Yam
E-mail: contato@dahliacapital.com.br
Endereço: Rua Joaquim Floriano, 940, Cj. 11, CEP 04534-004 - São Paulo - SP

V. SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

As medidas de segurança da informação e de cibersegurança utilizadas pela Dahlia Capital têm por finalidade assegurar que a infraestrutura física e tecnológica da Dahlia Capital é capaz de garantir a confidencialidade, integridade, privacidade e disponibilidade dos dados, incluindo Dados Pessoais tratados pela Dahlia Capital, e sistemas de informação utilizados no âmbito de suas atividades, além de minimizar as ameaças ao patrimônio, à imagem e aos negócios da Dahlia Capital e de seus Colaboradores, parceiros comerciais, investidores e terceiros com quem a Dahlia Capital se relaciona.

(i) Chefe de Segurança da Informação

A fim de aprimorar a governança sobre o tema da segurança da informação e cibersegurança na Gestora, o Subcomitê de Privacidade e Segurança da Informação (abaixo descrito) indicará, formalmente, um responsável sobre o tema (ora denominado "Chefe de Segurança da Informação" ou "CSO"), com mandato indeterminado. O Chefe de Segurança da Informação deverá, necessariamente, possuir senioridade compatível com a responsabilidade assumida, podendo ser um sócio da Gestora ou, em caso de empregado em regime CLT, possuir cargo de Gerente ou Diretor.

Dentre as responsabilidades assumidas pelo Chefe de Segurança da Informação da Gestora, estão:

- Definição e gerenciamento do programa de segurança da informação da Gestora, assegurando, no mínimo, o cumprimento do estabelecido na presente Política;
- Participação no Subcomitê de Privacidade e Segurança da Informação;
- Coordenação e acompanhamento de todas as ações, controles e mitigações a serem implementadas relativamente à segurança da informação na Gestora.

O Chefe de Segurança da Informação deverá, conforme necessidade, reportar periodicamente ao Comitê de Riscos e Compliance e ao Comitê Executivo temas relevantes relacionados à segurança da informação, tais como indicadores de risco cibernético e eventos relevantes, incidentes de segurança e status de planos de ação.

(ii) Subcomitê de Privacidade e Segurança da Informação

O Subcomitê de Privacidade e Segurança da Informação ("Subcomitê") constitui órgão interno auxiliar à DPO e ao Chefe de Segurança da Informação da Gestora para auxiliar na tomada de decisões relativas ao tema de Privacidade e Segurança da Informação. O Subcomitê se reúne, no mínimo, semestralmente e tem reporte direto ao Comitê de Risco e Compliance.

Compete ao Subcomitê:

- Implementar e coordenar uma abordagem em toda a companhia para os controles e procedimentos internos de privacidade e segurança da informação;
- Gerenciar eventuais solicitações de titulares de dados pessoais referentes a direitos previstos na LGPD;
- Estabelecer orientações quanto acesso a websites, aplicativos e/ou dispositivos, inclusive quanto a restrições temporárias ou permanentes que vierem a ser implementadas;
- Definir material de suporte padronizado para procedimento de avaliação de riscos;
- Solucionar e tomar decisões acerca dos procedimentos a serem tomados na ocorrência de um Incidente;
- Decidir sobre a contratação, quando necessário, de consultoria externa especializada; e
- Coordenar as comunicações entre a Dahlia Capital e autoridades, mídia, clientes, parceiros e Colaboradores no tema.

As reuniões do Subcomitê deverão ser formalizadas por meio de atas ou registros internos por escrito (i.e. e-mails com sumário executivo das discussões e deliberações), incluindo acompanhamento dos planos de ação definidos, conforme o caso.

(iii) Informações sigilosas

É terminantemente proibido aos Colaboradores copiar ou imprimir os arquivos utilizados, gerados ou disponíveis da Dahlia Capital para circulação em ambientes externos à empresa, sem a prévia e expressa autorização da Diretora de Riscos e *Compliance*/DPO. Isso porque tais arquivos poderão conter informações ou Dados Pessoais sigilosos, confidenciais e/ou sensíveis aos objetivos sociais da Dahlia Capital e que não poderão ser compartilhados com terceiros. As informações de caráter sensível ou confidencial da Gestora ou de terceiros, incluindo Dados Pessoais, serão armazenados em diretórios de rede, com *back up* em nuvem e controle de acesso gerido pelo DPO e pelo CSO da Dahlia Capital.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem comprovadamente realizadas estritamente no contexto da execução ou desenvolvimento das atividades e funções profissionais do Colaborador na Dahlia Capital. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e confidencialidade, responsabilizando-se também por seu extravio ou uso indevido. Ainda, qualquer impressão de documentos deve ser prontamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Dahlia Capital.

O descarte de informações sensíveis e/ou confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. O descarte de documentos físicos que contenham informações confidenciais e/ou sensíveis ou de suas cópias deverá ser realizado imediatamente após seu uso,

de maneira a evitar sua recuperação, sendo recomendável o seu descarte total, preferencialmente utilizando as máquinas trituradoras de papel disponibilizadas nos andares.

Adicionalmente, é proibida a utilização de pen-drives, discos de hard drive ou quaisquer outros meios para baixar ou gravar arquivos e documentos nos equipamentos e dispositivos corporativos, exceto se expressamente autorizado pela Diretora de Riscos e *Compliance*/DPO da Dahlia Capital mediante justificativa fundamentada. É proibida, ainda, a conexão de equipamentos na rede da Dahlia Capital que não estejam previamente autorizados pela Diretora de Riscos e *Compliance*/DPO da Dahlia Capital. A área de *Compliance* da Dahlia Capital implementará medidas e barreiras tecnológicas para garantir que tais restrições serão fielmente observadas.

(iv) Equipamentos corporativos

Todos os Colaboradores possuem equipamento pronto e configurado para utilização remota em caráter de *back up*, caso haja necessidade de atuar remotamente ou por motivo de problemas nos equipamentos na sede da Gestora. Novos equipamentos e/ou sistemas deverão ter suas configurações realizadas em ambientes de homologação.

Cada Colaborador é responsável por garantir a manutenção da segurança das informações armazenadas e disponibilizadas nos equipamentos corporativos sob sua responsabilidade, sujeitando-se ao cumprimento de todas as orientações de segurança da informação e cibernética, incluindo aquelas relativas a dupla autenticação de usuários para acesso a dispositivos e e-mail corporativo. Tal processo será auditável e rastreável eletronicamente pela área de TI/Desenvolvimento, sob a supervisão do Chefe de Segurança da Informação da Dahlia Capital.

(v) Sites e Downloads

O acesso a sites e *blogs* bem como o envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico, de cunho político ou de qualquer forma ofensivo também é terminantemente proibido, assim como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e afetar a reputação da Dahlia Capital, respondendo os responsáveis nos termos das políticas internas da Dahlia Capital e da legislação aplicável. No âmbito do exercício de suas atividades e funções profissionais na Dahlia Capital, todos os Colaboradores se comprometem a observar as orientações a qualquer tempo estabelecidas pelo DPO ou pelo CSO da Dahlia Capital quanto ao acesso a websites, aplicativos e/ou dispositivos, inclusive obrigando-se a respeitar restrições temporárias e permanentes que vierem a ser implementadas.

Programas instalados nos computadores, principalmente via internet (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia da Diretora de Riscos

e *Compliance*/DPO, além de avaliação de segurança pela empresa contratada para prover suporte de TI. Não é permitida, ainda, a instalação de nenhum software ilegal ou que possuam direitos autorais protegidos.

(vi) Acessos físicos e digitais

Os Colaboradores ou prestadores de serviços desligados da Dahlia Capital terão os seus acessos ao e-mail corporativo, às dependências físicas do escritório, aos sistemas (inclusive sistemas Web) e programas de propriedade da Dahlia Capital ou adquiridos de terceiros imediatamente bloqueados após a comunicação de saída de forma a preservar a confidencialidade, privacidade e integridade de informações confidenciais, reservadas ou privilegiadas de propriedade ou sob a guarda da Dahlia Capital, incluindo Dados Pessoais. A área de *Compliance* e Desenvolvimento, em conjunto com a empresa contratada para prover suporte de TI, sob a supervisão do CSO, mapearão os sistemas e programas ao qual o Colaborador desligado possuía acesso de forma a garantir que todos os bloqueios necessários foram efetuados com sucesso.

Da mesma forma, considerando que a Dahlia Capital mantém diferentes níveis de acesso a pastas e arquivos eletrônicos de acordo com as funções e senioridade dos Colaboradores, de forma que as combinações de login e senha são utilizadas para autenticar as pessoas autorizadas e conferir acesso à parte da rede da Dahlia Capital necessária ao exercício de suas atividades. Na hipótese de alteração de atividade de determinado Colaborador dentro da própria Dahlia Capital, este permanecerá com acessos exclusivamente aos dados e informações que precise para o desempenho de suas novas funções, incluindo os Dados Pessoais, conforme aplicável, e não terá mais acesso aos dados e informações que não sejam necessários para tanto.

Todo conteúdo que está na rede da Dahlia Capital poderá ser acessado conforme as restrições de acesso definidas pela área de *Compliance*. Arquivos pessoais salvos nos computadores, rede e dispositivos de propriedade da Dahlia Capital, incluindo e-mails corporativos, poderão ser acessados a qualquer tempo, caso necessário, pela área de *Compliance* da Dahlia Capital na medida do necessário para a consecução de monitoramento, investigações, auditoria e/ou para os devidos fins legais, ou em atendimento a determinações legais, regulatórias, judiciais ou administrativas.

O ambiente físico onde estão localizados os servidores da Dahlia Capital permanecerão a todo tempo sob acesso restrito e controlado. Caso necessário, o acesso a tais ambientes deverá ser requerido mediante solicitação fundamentada ao CSO que, por sua vez, avaliará a pertinência da solicitação. É recomendado que todos os acessos sejam feitos somente com o acompanhamento da empresa de suporte de TI. Vale destacar que as dependências físicas dos escritórios da Dahlia Capital são monitoradas via câmeras de segurança e que estas poderão ser verificadas em caso

de investigações, auditoria e/ou para os devidos fins legais, ou em atendimento a determinações legais, regulatórias, judiciais ou administrativas.

A Dahlia Capital conta com sistemas e ferramentas contratados para arquivamento, firewall, antivírus, *back up*, e linha de contingência, cuja configuração nos equipamentos corporativos só deve ser feita mediante acompanhamento técnico da empresa de suporte de TI.

(vii) Proteção de Dados Pessoais

A Dahlia Capital emprega medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, extravio, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito desses dados.

Entre as medidas de segurança adotadas, destacam-se as seguintes (além das medidas descritas no *item (vii) Ações de Proteção e Prevenção*): (i) armazenamento dos Dados Pessoais tratados em ambiente seguro; (ii) controle de acesso a Dados Pessoais armazenados no ambiente tecnológico da Dahlia Capital, de modo que apenas os Colaboradores que necessitem acessar tais dados para a consecução de suas atividades na Dahlia Capital o acessem, além de impedir o acesso de terceiros não autorizados; (iii) treinamento dos Colaboradores em temas de proteção de Dados Pessoais e segurança da informação; (iv) adoção das melhores práticas de segurança da informação, incluindo a realização de testes periódicos de verificação e elaboração de plano de resposta a incidentes de vazamento de Dados Pessoais; (v) manutenção de inventário com registros de atividades da Dahlia Capital que envolvam o tratamento de Dados Pessoais, estabelecendo as medidas necessárias para mitigar os riscos identificados em cada caso; e (vi) formalização de Termos de Privacidade e documentos similares com os Titulares e/ou outros Agentes de Tratamento dos Dados Pessoais.

Independentemente das medidas adotadas pela Dahlia Capital para evitar incidentes de segurança com dados e informações de sua propriedade e/ou de terceiros, é possível que ocorra algum problema motivado exclusivamente por um terceiro – como em caso de ataques de *hackers* ou *crackers* ou, ainda, em caso de culpa exclusiva do Titular, que ocorre, por exemplo, quando ele mesmo transfere seus dados a terceiro. Assim, embora a Dahlia Capital, em geral, seja responsável pelos Dados Pessoais que trata, ela se exime de responsabilidade caso ocorra uma situação excepcional sobre a qual não tenha nenhum tipo de controle ou ingerência.

De qualquer forma, caso ocorra qualquer tipo de incidente de segurança que possa gerar risco ou dano relevante para qualquer dos Titulares, Investidores, Usuários ou Colaboradores, a Dahlia Capital comunicará os afetados e a ANPD acerca do ocorrido, em conformidade com o disposto na LGPD.

(viii) Identificação e Avaliação de Riscos

A Dahlia Capital continuamente identifica, avalia e adota medidas para mitigar os principais riscos cibernéticos aos quais está exposta. No âmbito de suas atividades, a Dahlia Capital identificou os seguintes principais riscos internos e externos que precisam de proteção:

- a) Acesso indevido a dados e informações confidenciais: as informações confidenciais, sigilosas e sensíveis incluindo informações a respeito de investidores, clientes, Colaboradores, Dados Pessoais e informações da própria Dahlia Capital, operações e ativos investidos pelas carteiras de valores mobiliários sob sua gestão, e as comunicações internas e externas (por exemplo: correspondências eletrônicas e físicas);
- b) Falha nos sistemas de back-up;
- c) Contratação de Terceiros: falhas, danos ou erros causados por parte de prestadores de serviço contratados; e
- d) Ataques cibernéticos, conforme definido no Guia de Cibersegurança ANBIMA.

Ademais, o Guia de Cibersegurança ANBIMA definiu que os ataques mais comuns de criminosos cibernéticos são os seguintes:

- a) **Malware** – softwares desenvolvidos para corromper computadores e redes:
 - a. vírus: software que causa danos a máquina, rede, softwares e Banco de Dados;
 - b. cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
 - c. spyware: software malicioso para coletar e monitorar o uso de informações;
 - d. ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.
- b) **Engenharia social** – métodos de manipulação para obter informações confidenciais, como senhas, Dados Pessoais e número de cartão de crédito:
 - a. phishing: direciona o usuário para um site fraudulento, sem o seu conhecimento;
 - b. phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
 - c. vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
 - d. smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
 - e. acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.
- c) **Ataques de DDoS** (*Distributed Denial of Services*) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque

vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

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

Considerando todo o acima exposto, a Dahlia Capital entende que os seguintes níveis de risco e respectivos impactos (“Matriz de Risco”) devem ser observados:

Tabela 4 – Matriz de Risco			
Riscos	Probabilidade	Impacto	Nível de Risco
Acesso indevido a dados e informações confidenciais	Baixa	Alto	Médio
Falha nos sistemas de back-up	Baixa	Médio	Baixo
Falha de segurança cibernética por conta de Terceiros contratados	Baixa	Médio	Baixo
Ataques cibernéticos	Média	Alto	Alto

Considerando a Matriz de Risco, em conjunto com a empresa de suporte de TI, a Dahlia Capital continuamente conduz a avaliação de riscos de forma a identificar, avaliar e adotar medidas mitigadoras acerca dos riscos a que seus ativos tecnológicos relevantes estão expostos.

(ix) Ações de prevenção e proteção

A área de Riscos e *Compliance* e o Chefe de Segurança da Informação da Dahlia Capital, com o auxílio da empresa de suporte de TI, adota as ações de prevenção e proteção descritas nesta Política, dentre as quais destacamos:

- a) Controle de acessos aos ativos tecnológicos da Dahlia Capital, restringindo-os apenas àqueles que necessitam dos recursos para desempenho de suas atividades, incluindo diretório com matriz de acessos definida pela área de Riscos e *Compliance*;
- b) Restrição de acesso à infraestrutura física e aos servidores da Dahlia Capital com uso de fechadura externa digital (biometria) e/ou tradicional;
- c) Regras de acesso a dispositivos corporativos, com senhas individuais intrasferíveis e autenticação de múltiplos fatores para acesso a e-mail corporativo e acesso remoto à rede da Gestora via VPN;
- d) Rotina de instalação de atualizações nos softwares utilizados pela Dahlia Capital;

- e) Disponibilização de equipamentos corporativos com alto nível de segurança tecnológica para trabalho remoto por Colaboradores com proteção contra extravios, tendo em vista a criptografia de disco rígido em todos os notebooks;
- f) Serviço de *back up* com armazenamento diverso do local em que a rede da Dahlia Capital está localizada;
- g) Realização de diligência na contratação de serviços de terceiros, prezando, sempre que haja o compartilhamento de informações sigilosas, confidenciais ou sensíveis, pela celebração de acordo de confidencialidade e exigência de controles de segurança na própria estrutura dos Terceiros;
- h) Implementação de recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais;
- i) Diversos filtros de proteção nas contas de e-mail de todos os Colaboradores com aviso de atenção no caso de recebimento de e-mails de endereços não usuais, entre outras medidas;
- j) Restrição à instalação e execução de softwares e aplicações não autorizadas por meio de controles de execução de processos;
- k) Adoção de medidas para evitar vazamento de dados, incluindo Dados Pessoais, a terceiros não autorizados, incluindo restrição de uso de pen drives, instalação de softwares e aplicativos, utilização de software que impede armazenamento de anexos em dispositivos pessoais, etc;
- l) Monitoramento de tráfego de entrada e saída para identificação de atividade anormal rede em sites e bancos de dados;
- m) Detecção de intrusão em tempo real por meio de software projetado para identificar atividades de usuários não autorizados, ataques ou comprometimento de rede;
- n) Equipamentos de tecnologia sobressalentes para uso emergencial em caso de necessidade;
- o) Monitoramento do perímetro interno do escritório por meio de câmeras para segurança do data center e sala de servidores;
- p) Gestão de vulnerabilidades, incluindo aplicação periódica de atualizações de segurança (patches) em sistemas e softwares utilizados pela Gestora; e
- q) Manutenção de inventário atualizado de ativos tecnológicos, incluindo hardware e software.

(x) Monitoramento de terceiros

A contratação de prestadores de serviços terceiros para auxílio, suporte e envolvimento no tratamento de Dados Pessoais e/ou auxílio com a infraestrutura tecnológica da Dahlia Capital envolve determinados riscos que devem ser levados em consideração pelos Colaboradores envolvidos, demandando a adoção de cuidados proporcionais à atividade a ser desenvolvida pelo prestador de serviço e o risco relacionado.

Nesse sentido, a área de *Compliance* da Dahlia Capital deverá verificar, sob a supervisão do CSO, o conteúdo mínimo de *Compliance* em segurança cibernética de terceiros que (i) possuam acesso a informações e sistemas confidenciais ou sensíveis, (ii) prestem serviços de processamento, armazenamento de dados e de computação em nuvem, (iii) tenham conexões lógicas (*links*) com a Dahlia Capital, (iv) tratem Dados Pessoais coletados ou tratados pela Dahlia Capital na qualidade de Operadores ou subOperadores, ou (v) quaisquer outros que a área de *Compliance* julgue que por qualquer motivo possa gerar risco de privacidade ou de segurança da informação à Dahlia Capital, previamente à sua contratação, na forma do Anexo I desta Política.

Os serviços de processamento e armazenamento de dados e de computação em nuvem contratados pela Dahlia Capital são classificados como críticos, ou seja, de maior risco para as atividades da Dahlia Capital. Neste sentido, a Dahlia Capital deverá verificar a capacidade do potencial prestador de serviço, observado que esta verificação incluirá, no mínimo:

- I. o cumprimento da regulamentação em vigor;
- II. o acesso da Dahlia Capital aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- IV. a sua aderência a certificações exigidas pela Dahlia Capital para a prestação do serviço a ser contratado, caso aplicável;
- V. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- VI. a identificação e a segregação dos dados dos clientes da Dahlia Capital por meio de controles físicos ou lógicos; e
- VII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da Dahlia Capital.

O resultado será encaminhado à Diretora de Riscos e *Compliance*/DPO e ao CSO para avaliação da potencial contratação e dos riscos envolvidos, devendo a decisão sobre a contratação ficar formalizada, devendo ser periodicamente reavaliada.

A área Jurídica e de *Compliance* da Dahlia Capital deverá, na medida do praticável, envidar melhores esforços para formalizar a inclusão de cláusulas de proteção de Dados Pessoais e de requisitos de segurança da informação em contratos com prestadores de serviços e parceiros comerciais, bem como verificar a efetividade dos controles implementados por tal terceiro para atender aos requerimentos legais e regulatórios durante a vigência do relacionamento, na forma mencionada acima.

(xi) Treinamento de colaboradores

A área de *Compliance* da Dahlia Capital realizará treinamento em periodicidade anual (uma vez a cada ano), supervisionado pela Diretora de Riscos e *Compliance*/DPO e pelo CSO e, quando necessário e aplicável, pela empresa de suporte de TI, abrangendo todos os preceitos contidos na presente Política, de modo que todos os Colaboradores que tenham acesso a Dados Pessoais, informações confidenciais, sigilosas, reservadas, sensíveis ou privilegiadas, estejam sempre cientes e consonantes aos procedimentos de proteção e segurança das informações aqui previstos.

(xii) Testes periódicos de segurança da informação

A área de Riscos e *Compliance* da Dahlia Capital realizará, em periodicidade anual (uma vez a cada ano), sob a supervisão da Diretora de Riscos e *Compliance*/DPO e do CSO e com o auxílio da equipe de suporte de TI contratada, testes de sua infraestrutura tecnológica e sistemas de segurança de informação, bem como dos demais procedimentos contidos na presente política, a fim de averiguar e confirmar a efetividade das medidas adotadas e identificar eventuais incidentes. Em periodicidade definida pelo Comitê de Riscos e *Compliance*, a Gestora também poderá contratar consultor externo especializado para realizar avaliação do ambiente interno e externo de tecnologia da informação, através da execução de *scans* de vulnerabilidades.

Os resultados desses testes, bem como os procedimentos para saneamento de eventuais falhas ou fragilidades identificadas, serão descritos no Relatório Anual de *Compliance* da Dahlia Capital, que será arquivado na sede da Dahlia Capital sob a responsabilidade da Diretora de Riscos e *Compliance*.

As documentações relacionadas aos planos definidos e testes realizados, assim como os resultados auferidos e ações corretivas e mitigantes implementadas, deverão ser mantidas em diretório interno da área de *Compliance* e no CompliAsset como evidência em eventuais questionamentos internos ou de órgãos reguladores ou autorreguladores.

Os procedimentos e controles adotados pela Dahlia Capital para reduzir sua vulnerabilidade a incidentes e atender aos objetivos de segurança cibernética buscam abranger, sempre que possível: (i) mecanismos de criptografia aplicáveis a dispositivos e arquivos; (ii) mecanismos de autenticação para acesso às informações; (iii) ferramentas de prevenção de intrusões e de vazamento de informações, bem como de rastreabilidade de dispositivos corporativos; (iv) gestão de backups de segurança; (v) controles de acesso; (vi) proteção de redes; e (vii) monitoramento e restrição de acesso a sites e páginas de alto risco, definidos com o suporte da área de TI contratada, entre outros.

Os temas relacionados à segurança da informação e cibernética serão tratados no Comitê Trimestral de Riscos e *Compliance*, de forma ordinária, ou mesmo em reunião específica, em casos de eventos extraordinários, para que sejam tomadas medidas de recuperação, correção, limitação de danos, e respostas a incidentes de forma tempestiva.

VI. POLÍTICA DE BYOD

A Política de *Bring Your Own Device* (“**Política de BYOD**”) trata de regras e procedimentos específicos para a utilização de dispositivos pessoais de Colaboradores para acesso aos ativos da Dahlia Capital, com o objetivo de adotar práticas e rotinas de gestão, monitoramento e controles para identificar, avaliar e mitigar riscos, bem como para prevenir e tratar incidentes de segurança da informação. A Gestora disponibiliza uma série de equipamentos aos Colaboradores, para garantir que a utilização de dispositivos pessoais seja excepcional.

A Dahlia Capital permite o uso de celulares pessoais pelos colaboradores apenas para acesso aos e-mails corporativos e ao aplicativo Microsoft Teams. Qualquer outra forma de uso de dispositivos pessoais para acessar os ativos da Gestora deve ser previamente solicitada ao time de Legal & Compliance, que avalia a necessidade e os objetivos envolvidos e submete a decisão para aprovação da Diretora de Risco e Compliance.

A Dahlia Capital adota modelo de **confiança zero** para o acesso de dispositivos pessoais aos ativos corporativos. Isso significa que a Gestora (i) concede acesso aos dispositivos pessoais somente em casos necessários, desde que seja adicionada dupla autenticação, e após autorização expressa da Diretora de Risco e Compliance; e (ii) não presume confiança em nenhum dispositivo externo.

A Dahlia Capital não permite o acesso de dispositivos externos não autorizados aos arquivos e sistemas internos não indicados anteriormente. No momento da contratação, todos os Colaboradores recebem dispositivos corporativos, notebooks e/ou CPUs, destinados ao acesso aos sistemas da Gestora. Esses dispositivos são configurados com *Virtual Private Network* (VPN), que permite o acesso remoto seguro aos arquivos e sistemas internos exclusivamente a partir de equipamentos autorizados.

O time de Legal & Compliance busca implementar ações e rotinas de conscientização voltadas aos principais temas relevantes para as atividades da Gestora, com foco no acesso de dispositivos externos aos arquivos e sistemas internos. Essas iniciativas visam promover o entendimento, por parte dos Colaboradores, sobre as responsabilidades individuais, controles de segurança, boas práticas e medidas de conformidade aplicáveis ao uso de dispositivos externos.

Considerando os riscos, exigências regulatórias e políticas internas, a Dahlia Capital busca:

- i. Garantir que os Colaboradores compreendam suas responsabilidades individuais e corresponsabilizações ao optarem pelo uso de dispositivos pessoais para acessarem ativos da organização (i.e. e-mail e Microsoft Teams);
- ii. Garantir que os Colaboradores compreendam a abrangência dos controles e acessos franqueados à organização em decorrência da opção pela utilização de dispositivos pessoais para acessar ativos corporativos;
- iii. Garantir que os Colaboradores compreendam os potenciais impactos que práticas e controles para mitigação de riscos realizados pela organização podem gerar ao dispositivo pessoal;
- iv. Estimular a incorporação de práticas de segurança no uso de dispositivos pessoais pelos colaboradores para acessar ativos corporativos e atitudes éticas, que zelem pela segurança da informação e cibernética e a conformidade com as políticas, regras e procedimentos da organização.

Caso opte por utilizar seus próprios dispositivos para acesso ao e-mail corporativo e ao Microsoft Teams, o Colaborador reconhece e assume a responsabilidade por eventuais incidentes de segurança decorrentes dessa utilização, comprometendo-se a reportar imediatamente quaisquer irregularidades e/ou perda do dispositivo ao time de Legal & Compliance. A Dahlia Capital, por sua vez, assegura a transparência na descrição dos controles implementados e na comunicação dos potenciais impactos relacionados a incidentes de segurança, bem como a pronta adoção de medidas de resposta, investigação e, quando aplicável, aplicação das sanções cabíveis ao Colaborador envolvido.

Os Colaboradores autorizados a utilizar seus dispositivos pessoais para acesso à quaisquer Informações Confidenciais da Dahlia Capital receberão um Termo de Uso de Dispositivos Pessoais para acesso a ativos da Gestora, que conterà, no mínimo:

- I. Quais acessos serão concedidos ao Colaborador, abrangendo informações, dados, mídias e arquivos;
- II. Potenciais incidentes relacionados ao dispositivo pessoal;
- III. Permissões e proibições;
- IV. Requisitos mínimos para acesso, reprodução, tratamento, transporte, compartilhamento e descarte de dados da gestora através de dispositivos pessoais, abrangendo a utilização de redes corporativas de dados e de computação em nuvem;
- V. Procedimentos para o Colaborador reportar casos de perda, danificação, roubo ou furto dos dispositivos pessoais utilizados para acessar ativos da Gestora;
- VI. Situações elegíveis à revogação de acesso e apagamento remoto de dados corporativos pela organização, abrangendo a situação de desligamento do Colaborador; e

- VII. Medidas disciplinares para situações de não conformidade ou violação do termo de uso pelos colaboradores.

A Dahlia Capital poderá, por decisão fundamentada do Subcomitê de Privacidade e Segurança da Informação, adotar soluções de gerenciamento de dispositivos ou aplicações móveis (*Mobile Device Management/Mobile Application Management*), com o objetivo de proteger dados corporativos acessados por dispositivos pessoais, sem acesso a dados pessoais dos Colaboradores. Os Colaboradores, desde já, consentem com a instalação e manutenção de referidas soluções (*softwares* ou aplicativos) em seus dispositivos pessoais aptos a acessarem ativos ou dados corporativos. A Gestora poderá, quando aplicável, realizar a exclusão remota de dados corporativos (*remote wipe*), nos termos do Termo de Uso de Dispositivos Pessoais.

A Dahlia Capital poderá prever procedimentos de contingência específicos para tratamento de incidentes de segurança da informação envolvendo todos os dispositivos utilizados pelos Colaboradores, abrangendo identificação, contenção, mitigação de impactos e comunicação às autoridades competentes, quando aplicável.

VI. POLÍTICA DE SENHAS

A Política de Senhas dispõe sobre recomendações e procedimentos a serem observados por todos os Colaboradores da Dahlia Capital na criação, utilização e manutenção de senhas. Todos os Colaboradores da Dahlia Capital deverão utilizar senhas de acesso individuais para seus dispositivos corporativos e, quando aplicável, para dispositivos pessoais autorizados, nos termos da Política de BYOD.

Nesse contexto, a Dahlia Capital recomenda que:

- (i) as senhas sejam criadas observando padrão de complexidade adequado, com, no mínimo, 10 (dez) caracteres, contemplando a combinação de caracteres alfabéticos, numéricos e especiais (símbolos);
- (ii) as senhas sejam alteradas, no mínimo, a cada 90 (noventa) dias para Colaboradores em geral e, para Colaboradores com perfil de Administrador, no mínimo a cada 45 (quarenta e cinco) dias;
- (iii) as senhas não sejam reutilizadas, de modo que não se repitam aquelas anteriormente utilizadas, ou padronizadas para todos os dispositivos e contas; e
- (iv) sejam utilizados mecanismos de autenticação em dois fatores e outras formas de autenticação para reforço da segurança, tais como recursos biométricos, conforme a necessidade e a definição do Subcomitê de Privacidade e Segurança da Informação em cada caso.

Com o objetivo de assegurar o cumprimento das diretrizes estabelecidas nesta Política, a Gestora poderá implementar soluções tecnológicas que reforcem automaticamente os requisitos mínimos de segurança

aplicáveis às credenciais de acesso, incluindo, mas não se limitando, ao bloqueio da criação de senhas que não atendam aos padrões de complexidade, histórico e periodicidade definidos. Adicionalmente, a Gestora poderá adotar ferramentas corporativas de gerenciamento seguro de senhas (password managers), bem como outras soluções tecnológicas voltadas à autenticação e proteção de acessos, com o intuito de elevar o nível de segurança dos dispositivos, aplicações e sistemas utilizados por seus Colaboradores, em linha com as melhores práticas de mercado.

VI. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada no mínimo uma vez a cada ano e será devidamente atualizada caso, por questões regulatórias ou internas, seja constatada a necessidade de alteração do seu conteúdo. A Política poderá, ainda, ser alterada/atualizada a qualquer tempo em razão de circunstâncias que demandem tal providência.

A Dahlia Capital se reserva o direito de modificar, a qualquer momento, o capítulo de Privacidade e Proteção de Dados Pessoais da presente Política, especialmente para adaptá-lo a eventuais alterações feitas no Site Dahlia e/ou na regulamentação em vigor. As alterações se darão através de comunicação a Usuários por meio de atualização a ser disponibilizada no Site Dahlia. O acesso e utilização do Site Dahlia ou aplicação nos Fundos após a publicação das alterações implicará aceitação automática e imediata aos novos termos da Política. A Dahlia Capital recomenda a verificação periódica do Site Dahlia para leitura e ciência desta Política de atualizada.

ANEXO I**MODELO DE TERMO DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO
PARA TERCEIROS**

Razão Social: Clique ou toque aqui para inserir o texto. ("Instituição")

CNPJ: Clique ou toque aqui para inserir o texto.

E-mail para correspondência: Clique ou toque aqui para inserir o texto.

Ao completar esse checklist e assinalar as declarações abaixo, o responsável pelo preenchimento do documento, como representante da Instituição, atesta que toda a documentação solicitada foi enviada e que as informações lá contidas e as declarações feitas neste documento são verdadeiras na data em que esse termo foi preenchido.

DOCUMENTOS

Política de Segurança da Informação	Escolher um item.
Política de Privacidade e/ou Proteção de Dados Pessoais	Escolher um item.
Certificações relacionadas (ex.: ISO, EXIN)	Escolher um item.

DECLARAÇÕES

Declaro que possuo procedimentos, políticas, programa e procedimentos formais relativos à proteção de dados, segurança da informação e cibersegurança adequados para garantir o cumprimento de toda a legislação e regulamentação aplicável à proteção de Dados Pessoais (incluindo autorregulamentação), incluindo, mas não se limitando à LGPD e eventuais guias de orientação e normas publicadas pela ANPD e ANBIMA, conforme aplicável.	Escolher um item.
A Instituição declara que possui as 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 qualquer forma de Tratamento inadequado ou ilícito.	Escolher um item.
Declaro que a Instituição realiza treinamentos, ações de conscientização, entre outros, voltados para a temática de proteção de Dados Pessoais e de segurança da informação junto a seus funcionários.	Escolher um item.
Declaro que possuo plano de respostas a incidentes e remediação capaz de identificar os riscos relacionados e aplicar medidas de forma a reverter ou mitigar os efeitos do incidente, além da comunicação apropriada a clientes e reguladores, quando aplicável.	Escolher um item.

Caso não possua alguns dos documentos solicitados ou não esteja de acordo com alguma das declarações acima, por favor, explique sua motivação e dê mais detalhes abaixo:

Clique ou toque aqui para inserir o texto.

Data de preenchimento:

Clique ou toque aqui para inserir uma data.

Responsável por preencher o termo:

Clique ou toque aqui para inserir o texto.

ANEXO II

PLANO DE RESPOSTA À INCIDENTES DE SEGURANÇA E PRIVACIDADE

O presente Anexo visa dar transparência às principais diretrizes adotadas pela Dahlia Capital em seu Plano de Resposta a Incidentes de Segurança e Privacidade. A Dahlia Capital mantém exclusivamente interno seu Plano de Resposta a Incidentes de Segurança e Privacidade (“PRI”), elaborado pela área de Riscos e *Compliance* da Gestora sob a supervisão da Diretora de Riscos e *Compliance*/DPO e com o envolvimento/aprovação de seu Comitê Executivo, o qual é arquivado na sede da Dahlia Capital e disponibilizado a todos os seus Colaboradores.

Um “**Incidente**” nos termos do Plano de Resposta a Incidentes de Segurança e Privacidade, é qualquer evento adverso, eminente ou confirmado, relacionado a acesso não autorizado, interrupção, mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida, apropriação, disseminação, publicação indevida de informação protegida de algum ativo de informação crítico ou, ainda, relacionado à violação na segurança de Dados Pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos Dados Pessoais.

(i) **Papéis e Responsabilidade**

A Diretora de Riscos e *Compliance*/DPO é o responsável pela implementação e monitoramento das respostas a Incidentes ocorridos no ambiente de tecnologia da Dahlia Capital.

A Diretora de Riscos e *Compliance*/DPO tem como responsabilidade:

- Implementar e atualizar, sempre que necessário, o PRI da Dahlia Capital, envidando esforços para que esta satisfaça as necessidades da Dahlia Capital e esteja em conformidade com a regulamentação vigente.
- Receber relatórios sobre Incidentes e tomar medidas para que tais Incidentes reportados sejam prontamente endereçados e solucionados, em conjunto com o Comitê Extraordinário de Incidentes da Dahlia Capital, quando aplicável.
- Supervisionar periodicamente a conformidade do PRI com o objetivo de aprimorar processos e garantir efetividade na resposta a Incidentes.
- Desenvolver, implementar e manter procedimentos e mecanismos automatizados para o acompanhamento e registro de Incidentes.

O Comitê Executivo tem como responsabilidade:

- Determinar a alocação de recursos apropriados para a proteção das informações da Dahlia Capital, levando em consideração análise baseada em risco e as prioridades organizacionais da Dahlia e os incidentes que tenham sido eventualmente identificados anteriormente; e
- Aprovação final do PRI.

O Subcomitê de Privacidade e Segurança da Informação tem como responsabilidade:

- Solucionar e tomar decisões acerca dos procedimentos a serem tomados no evento de um Incidente;
- Decidir sobre a contratação, quando necessário, de consultoria externa especializada; e
- Coordenar as comunicações entre a Dahlia Capital e autoridades, mídia, clientes, parceiros e Colaboradores.

Todos os Colaboradores estão instruídos a reportar qualquer Incidente, seja ele um Incidente concreto ou suspeito, diretamente à Diretora de Riscos e *Compliance*/DPO imediatamente após a sua identificação ou suspeita de ocorrência. Incidentes serão registrados e arquivados na sede da Dahlia Capital por meio de relatório de avaliação pós-incidente (“Relatório Pós-Incidente”) e no Relatório Anual de Compliance da Dahlia Capital.

(ii) Estágios do PRI

A Dahlia manterá um Plano de Resposta à Incidentes (“PRI”) que endereça os diferentes estágios relacionados a um Incidente de Segurança da Informação, sendo eles:

- I. Preparação
- II. Prevenção
- III. Reporte
- IV. Avaliação
- V. Contenção
- VI. Erradicação
- VII. Recuperação
- VIII. Comunicação
- IX. Acompanhamento pós-incidente

(iii) Incidente de Segurança com Dados Pessoais

Um Incidente de Segurança com Dados Pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de Dados Pessoais tratados pela Dahlia Capital, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, que possa

ocasionar risco para os direitos e liberdades do respectivo Titular (“**Incidente com Dados Pessoais**”).

No caso de um Incidente com Dados Pessoais, a Diretora de Riscos e *Compliance/DPO*, em conjunto com consultoria de TI especializada, irá avaliar internamente questões adicionais, incluindo, a vulnerabilidade que for explorada no evento, meio pelo qual foram obtidos os Dados Pessoais, categoria de Dados Pessoais objeto do Incidente, extensão do vazamento, impacto ao Titular, e Impacto Reputacional, de forma a concluir sobre a existência de risco ou dano relevantes aos Titulares. Os incidentes deverão ser classificados de acordo com sua criticidade, considerando, entre outros fatores, o volume de dados afetados, a sensibilidade das informações e o impacto regulatório.

Nos casos em que a Dahlia Capital atua como Controladora, a Diretora de Riscos e *Compliance/DPO* prontamente comunicará a ANPD e o Titular acerca da ocorrência do Incidente com Dados Pessoais, nos termos da LGPD e demais regulações aplicáveis. Quando a Dahlia Capital atuar como Operadora, a Diretora de Riscos e *Compliance/DPO* comunicará ao respectivo Controlador dos Dados Pessoais afetados e adotará todas as medidas cabíveis para colaborar com o Controlador na remediação do incidente e dos danos causados aos Titulares.

A Dahlia Capital adotará sempre uma postura conservadora quanto à comunicação acima referida à ANPD e ao Controlador dos Dados Pessoais afetados, de modo que a comunicação será realizada mesmo nos casos em que houver dúvida sobre a existência de riscos ou danos aos envolvidos.

(iv) Comunicação à ANPD

No caso de comunicação à ANPD, a Diretora de Riscos e *Compliance/DPO* elaborará, em até 3 (três) dias úteis, ressalvada a existência de prazo para comunicação previsto em legislação específica, contados da data do conhecimento do Incidente com Dados Pessoais, relatório claro e conciso contendo, no mínimo:

- a descrição da natureza e da categoria dos Dados Pessoais afetados;
- o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- os motivos da demora, no caso de a comunicação não ter sido realizada no prazo indicado;
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

- a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;
- os dados do encarregado ou de quem represente o controlador;
- a identificação do operador;
- a identificação do operador, quando aplicável;
- a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
- o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Com base no relatório, será preenchido o [Formulário Eletrônico](#) disponibilizado pela ANDP e o documento será peticionado nos meios apropriados.

(v) Comunicação ao Titular

No caso de comunicação ao Titular, a Diretora de Riscos e *Compliance*/DPO elaborará, em até 3 (três) dias úteis, contados da data do conhecimento do Incidente com Dados Pessoais, relatório claro e conciso, com linguagem simples e de fácil entendimento, enviados de forma direta e individualizada, se possível, contendo, no mínimo:

- a descrição da natureza e da categoria de dados pessoais afetados;
- as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- os motivos da demora, no caso de a comunicação não ter sido feita no prazo indicado;
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
- a data do conhecimento do incidente de segurança; e
- o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os Titulares afetados, a ocorrência do incidente será comunicada, no prazo e com as informações definidas acima, pelos meios de divulgação disponíveis, como seu site, mídias sociais e canais de atendimento ao titular, permitindo o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.