Política de Privacidade de Dados Pessoais do ChildFund Brasil

1. OBJETIVO

Esta Política de Privacidade de Dados Pessoais ("Política" ou "Política de Privacidade") tem como objetivo estabelecer normas e diretrizes sobre o tratamento de dados pessoais coletados pelo ChildFund Brasil ("ChildFund Brasil"), conforme regulamentação aplicável.

Ao consentir com essa Política de Privacidade, o titular concorda com os termos nela descritos e com o tratamento de dados pessoais, para os fins descritos neste documento.

2. ABRANGÊNCIA

A presente Política é aplicável às atividades que envolvam o tratamento de dados pessoais e abrange todos os websites, portais, aplicativos e formulários do ChildFund Brasil.

3. TERMOS E DEFINIÇÕES

Para o entendimento desta política devemos considerar as definições e terminologias conforme o detalhamento a seguir:

Agentes de tratamento: o controlador e o operador.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Autoridade Nacional / Autoridade Nacional de Proteção de Dados (ANPD): Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados ("LGPD") em todo o território nacional.

Banco de Dados: conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Colaboradores: pessoas contratadas para integrar o quadro de funcionários do ChildFund Brasil.

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.

Cookies: arquivos que contêm pequenas partes de dados que são compartilhados entre um dispositivo tecnológico e um servidor web com intuito de tornar a navegação mais amigável e melhorar a experiência do usuário.

Dado Anonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de anonimização na ocasião de seu tratamento.

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.

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.

Encarregado pelo Tratamento de Dados Pessoais ("Encarregado") / DPO (Data Protection Officer): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Finalidade: motivo pelo qual é realizado o tratamento do dado pessoal do titular.

Lei Geral de Proteção de Dados Pessoais (LGPD): a Lei nº 13.709/2018 ou LGPD, que dispõe sobre o tratamento de dados pessoais de pessoas naturais, independente do meio, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Opt-In: manifestação do titular em expressar, prévia e explicitamente, seu consentimento para recebimento de comunicação específica ou autorização para tratamento de dados pessoais.

Opt-Out: O oposto ao *opt-in*, ou seja, a revogação de um consentimento previamente realizado.

Órgão de Pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Site / Website: endereço virtual de pessoa física ou jurídica, composto por um conjunto de páginas eletrônicas.

Titular / Usuário: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência Internacional de Dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.

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.

Uso Compartilhado de Dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

4. SOBRE A FINALIDADE DE TRATAMENTO DOS DADOS PESSOAIS

Os dados pessoais tratados pelo ChildFund Brasil têm como objetivo atender diversas finalidades, a depender do relacionamento do titular com o ChildFund Brasil. Assim, apresentamos abaixo, de forma não exaustiva, as principais hipóteses em que trataremos as informações pessoais do titular:

- Para o cumprimento de obrigação legal (art.7°., II da LGPD): quando decorrente de determinação legal e/ou regulatória impostas ao ChildFund Brasil.

- Na necessidade para execução contratual (art. 7°., V da LGPD): cumprimento de contratos específicos pelo ChildFund Brasil junto a diversas empresas (fornecedores e/ou prestadores de serviço).

- Para a elaboração, monitoramento de programas e projetos sociais, viabilização de doações e apadrinhamentos financeiros a crianças, e demais contratos ou diligências preliminares;
    - Relacionamento e oferecimento de informações relacionadas aos programas e projetos do ChildFund Brasil;
    - Cadastro para acesso às plataformas do ChildFund Brasil;
    - Atendimentos específicos realizados pelo ChildFund Brasil;
    - Fornecimento de suporte aos usuários, doadores, funcionários, fornecedores, prestadores de serviços e pessoas que apadrinharam ou desejam apadrinhar crianças.

- Para o exercício regular de direitos em processo judicial, administrativo ou arbitral;
    - Na condução dos processos de recebimento de reclamações em Ouvidorias;
    - No recebimento e elaboração de respostas a reclamações e processos junto a órgãos públicos;
    - No armazenamento de informações para defesa em processos judiciais, administrativos ou arbitrais.

- Na persecução do interesse legítimo do ChildFund Brasil, sempre no limite de sua expectativa, e nunca em prejuízo de interesses, direitos e liberdades fundamentais do titular;

- Por meio de autorização concedida pelo titular (“Consentimento”)

A base de dados formada por meio da coleta e armazenamento de dados pessoais do titular é de propriedade e responsabilidade do ChildFund Brasil, sendo que seu

uso, acesso e compartilhamento, quando necessários, serão realizados dentro dos limites e propósitos de seus negócios, podendo, neste sentido, serem disponibilizados para consulta, compartilhados e cedidos a fornecedores e autoridades, desde que obedecido ao disposto na presente Política de Privacidade e na regulamentação aplicável.

Nenhum documento, informação e/ou dado pessoal será divulgado e/ou compartilhado em nenhuma hipótese, exceto se expressamente autorizado pelo usuário, para fins de cumprimento dos serviços contratados ou mediante ordem judicial ou por determinação legal.

Poderá ser necessário que sejam transmitidos os dados pessoais do usuário a outra entidade do ChildFund Brasil, um parceiro ou prestador de serviços externo. O ChildFund Brasil exige que seus prestadores de serviço tratem tais dados apenas em conformidade com esta Política de Privacidade e com a regulamentação aplicável.

Internamente, os dados dos usuários são acessados somente por colaboradores devidamente autorizados, respeitando os princípios de finalidade, adequação, necessidade e demais princípios inerentes ao tratamento de dados pessoais, sempre para os objetivos do ChildFund Brasil, além do compromisso de confidencialidade e preservação da privacidade nos termos desta Política de Privacidade.

5. TIPOS DE TITULARES DE DADOS PESSOAIS

Os titulares dos dados pessoais tratados pelo ChildFund Brasil são categorizados da seguinte forma:

- Usuários;
- Doadores;
- Crianças;
- Colaboradores;
- Dependentes;
- Fornecedores;
- Prestadores de Serviços;
- Padrinhos;
- Madrinhas;
- Candidatos a cargos e funções no ChildFund Brasil;
- Conselheiros;
- Interessados.

6. DADOS COLETADOS

Para que o ChildFund Brasil realize seu fim social, torna-se imprescindível a coleta de algumas informações sobre o titular. Desta forma, poderão ser coletados dados pessoais fornecidos diretamente pelo titular, seus responsáveis legais (mediante consentimento específico autorizando o tratamento de dados pessoais de criança), empresas, por terceiros ou coletados de forma automática, de acordo com a elaboração, monitoramento de programas e projetos sociais, viabilização de doações e apadrinhamentos financeiros a crianças ou qualquer outro tipo de relacionamento do titular com o ChildFund Brasil. Veja abaixo as formas de coleta de dados pessoais:

Dados pessoais fornecidos diretamente pelo titular: Serão coletados todos os dados pessoais inseridos ou encaminhados ao acessar um dos nossos canais (portais ou aplicativos) do ChildFund Brasil.

Dados pessoais fornecidos por empresas: visando exclusivamente o cumprimento de obrigação legal (art.7°., II da LGPD) ou quando necessários à execução de contratos e/ou procedimentos preliminares em que o titular faça parte (art.7°., V da LGPD).

Dados pessoais fornecidos por terceiros: O ChildFund Brasil pode receber dados pessoais por intermédio de terceiros, sejam parceiros, doadores, padrinhos, madrinhas ou prestadores de serviços, que possuam algum relacionamento com o titular. É possível, ainda, que o ChildFund Brasil colete dados de bases públicas, disponibilizados por autoridades (como a Receita Federal, por exemplo) ou por terceiros, ou até mesmo dados tornados públicos pelo titular em websites ou redes sociais, sempre respeitando a privacidade.

Dados pessoais coletados automaticamente: o ChildFund Brasil também pode coletar uma série de informações de modo automático e para tanto se utiliza de algumas tecnologias de mercado (cookies por exemplo), com o propósito de melhorar a experiência de navegação do usuário em portais e aplicativos do ChildFund Brasil, de acordo com os seus hábitos e preferências.

Para toda a coleta de dados pessoais, sempre serão seguidas as seguintes regras essenciais:

- Apenas serão coletadas informações imprescindíveis para a elaboração, monitoramento de programas e projetos sociais, viabilização de doações e apadrinhamentos financeiros a crianças;
- Se necessário, pediremos autorização ou avisaremos ao titular para coleta de novos dados, acompanhado da devida justificativa;
- Os dados pessoais coletados somente serão utilizados para cumprir com as finalidades informadas ao titular.

O tratamento de dados pessoais de crianças e adolescentes será realizado apenas mediante consentimento específico e destacado de um dos pais ou do responsável legal.

Os dados tratados pelo ChildFund Brasil serão armazenados pelo tempo necessário para atendimento das finalidades às quais foram coletados ou, ainda, para cumprimento de requisitos legais e regulatórios. Findo o prazo de retenção dos dados ou quando solicitado pelo titular, o ChildFund Brasil os eliminará de maneira segura.

7. COMPARTILHAMENTO DE DADOS COM TERCEIROS

Os dados pessoais tratados pelo ChildFund Brasil poderão ser acessados por terceiros, conforme a seguir definido.

Para os nossos objetivos

O ChildFund Brasil poderá compartilhar dados com terceiros para os seus próprios objetivos. O ChildFund Brasil compartilhará os dados pessoais estritamente necessários para prover ou de cumprir seu objeto social, bem como para diversos objetivos internos, tais como para elaboração, monitoramento de programas e projetos sociais, viabilização de doações e apadrinhamentos financeiros a crianças, além de assegurar a segurança das doações e melhorar a qualidade das ações executadas pelo ChildFund Brasil.

Para razões estratégicas

O ChildFund Brasil poderá compartilhar todas as categorias de dados listadas no item 6 com parceiros e outras entidades que fornecem ao ChildFund Brasil certos serviços ou auxiliam com funções internas, como análise de dados, manutenção da segurança de sistemas internos, ou assegurar o cumprimento de disposições legais. Por exemplo, o ChildFund Brasil poderá compartilhar informações com empresas de auditoria, escritórios de advocacia para obter assistência jurídica, escritórios de contabilidade ou com outros profissionais. Outras entidades que possam receber dados pessoais para tais propósitos incluem fornecedores de serviços de segurança da informação, empresas de análise de dados, avaliadores de garantia de qualidade, dentre outros.

Por razões legais e regulamentares

O ChildFund Brasil poderá compartilhar todas as categorias de dados pessoais informadas no item 6 com parceiros, prestadores de serviços e outras entidades quando necessário para cumprir com obrigações legais ou regulamentares, incluindo o cumprimento a qualquer lei aplicável, processo judicial ou administrativo. O ChildFund Brasil também poderá compartilhar informações para proteger e defender os direitos do Grupo, titulares de dados pessoais, ou qualquer outra pessoa, para proteger contra atividades fraudulentas ou maliciosas, para fazer cumprir os Termos e Condições do ChildFund Brasil, ou para cooperar com agências fiscalizadoras da lei.

Quando o titular consente com a divulgação

O ChildFund Brasil poderá compartilhar certas informações com parceiros ou outras entidades quando o titular instrui a compartilhar ou de outra forma consentir em compartilhar essas informações, sendo que todo consentimento manifestado pelo titular deverá ser prévio e expresso.

8. SOBRE OS DIREITOS E REQUERIMENTOS DOS TITULARES

Em conformidade com a regulamentação aplicável, o ChildFund Brasil assegura os seguintes direitos ao titular:

- A confirmação da existência de tratamento;
- O acesso aos seus dados;
- A correção de dados incompletos, inexatos ou desatualizados;

- A anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a regulamentação aplicável;
- A portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD;
- A eliminação dos dados pessoais tratados com o consentimento do titular, com exceções previstas na regulamentação aplicável;
- A informação das entidades públicas e privadas com as quais o ChildFund Brasil realizou uso compartilhado de dados;
- A informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- A revogação do consentimento, nos termos da regulamentação aplicável;
- Revisão de decisões automatizadas.

Os direitos dos titulares previstos na regulamentação aplicável e nesta Política poderão ser exercidos mediante a requisição expressa por parte do titular ou do representante legal e poderá ser realizada através do canal de relacionamento disponível no portal de privacidade ou no aviso de privacidade.

O usuário fica ciente, por meio deste documento, que eventual solicitação de exclusão de informações essenciais para a gestão de seu cadastro junto ao ChildFund Brasil, quando passível de aplicação, implicará no término de sua relação contratual/negocial.

O ChildFund Brasil empreenderá todos os esforços razoáveis para atender as requisições feitas pelo titular, no menor tempo possível. No entanto, fatores justificáveis, poderão atrasar ou impedir o seu rápido atendimento, sendo certo que, em caso de demora, será apresentado ao titular os devidos motivos.

Cabe ao titular o dever de prestar informações corretas e atualizadas. O ChildFund Brasil não é responsável pela precisão, veracidade ou falta dela nas informações prestadas podendo a seu critério suspender e/ou cancelar o cadastro do usuário a qualquer momento, caso seja identificada qualquer inexatidão.

Por fim, o titular deve estar ciente que a sua requisição poderá ser legalmente rejeitada, seja por motivos formais (a exemplo de sua incapacidade de comprovar sua identidade) ou legais (a exemplo do pedido de exclusão de dados cuja manutenção é livre exercício de direito pelo ChildFund Brasil), sendo certo que, na hipótese de impossibilidade de atendimento destas requisições, será apresentado ao titular as justificativas razoáveis.

9. SOBRE A SEGURANÇA

Qualquer dado pessoal em posse do ChildFund Brasil será armazenado de acordo com os mais rígidos padrões de segurança adotados pelo mercado, o que inclui a adoção de medidas como:

- Proteção contra acesso não autorizado;

- Acesso restrito de pessoas ao local onde são armazenadas as informações pessoais;

- Adoção de procedimentos junto aos colaboradores, prestadores de serviço e fornecedores que realizarem o tratamento de dados pessoais no sentido de se comprometerem em manter o sigilo absoluto das informações, adotando as melhores práticas para manuseio destes dados, conforme determinado nas políticas e procedimentos corporativos.

Além dos esforços técnicos, o ChildFund Brasil também adota medidas institucionais visando a proteção de dados pessoais, de modo que mantém programa de governança e privacidade aplicado às suas atividades e estrutura de governança, constantemente atualizado.

De qualquer forma, na remota hipótese de incidência de episódios desta natureza, o ChildFund Brasil garante o pleno esforço para remediar as consequências do evento, sempre garantindo a devida transparência ao titular.

10. SOBRE LINKS PARA OUTROS SITES

O ChildFund Brasil poderá disponibilizar links para outros sites considerados pertinentes, convênios corporativos ou devido a imposição regulamentar, judicial ou administrativa. Cabe ressaltar que o ChildFund Brasil não se responsabiliza pela política de privacidade praticada por estes sites. Os terceiros têm sua própria política para a coleta, uso, compartilhamento e qualquer espécie de tratamento de dados relacionados com os serviços destes terceiros e caberá a estes terceiros a devida manutenção dos dados. O ChildFund Brasil recomenda a leitura das políticas destes terceiros.

11. SOBRE COOKIES

Cookies são arquivos que podem ser armazenados no dispositivo do usuário, contendo pequenas partes de dados que são compartilhados quando um dispositivo visita ou utiliza os serviços on-line do ChildFund Brasil.

As informações coletadas, geralmente o nome do site que o originou, seu tempo de vida e um valor gerado aleatoriamente, são interpretadas e executadas pelos portais ou aplicativos do ChildFund Brasil, o que possibilita o reconhecimento do usuário e identificação futura de seus interesses e necessidades.

TIPOS DE COOKIES	O QUE ELES FAZEM?
NECESSÁRIOS	Cookies essenciais para que o portal ou aplicativo visitado funcione corretamente. Este tipo de cookie não armazena informação pessoal identificável e geralmente são configurados em resposta a uma solicitação de serviços do usuário, tais como definir as suas preferências de privacidade, iniciar sessão ou preencher formulários. Este tipo de cookie não pode ser desativado em portais e aplicativos do ChildFund Brasil, podendo o usuário configurar o seu navegador para bloqueá-los. Entretanto, cabe ressaltar que esta ação impactará algumas funcionalidades dos portais e aplicativos.
DESEMPENHO	Cookies que permitem contabilizar visitas e fontes de tráfego, visando medir e aprimorar o desempenho dos nossos portais e aplicativos. Todas as informações coletadas por este tipo de cookie são anônimas. O usuário pode proibir a execução destes cookies, mas o ChildFund Brasil ficará impossibilitado de entender como o usuário interage com

	os portais e aplicativos, sem fornecimento de informações sobre as áreas visitadas, o tempo de visita e quaisquer problemas encontrados, como mensagens de erro, por exemplo.
FUNCIONALIDADE	Cookies que permitem ao portal ou aplicativo memorizar as escolhas do usuário, proporcionando uma experiência personalizada. Podem ser estabelecidos pelo ChildFund Brasil ou por fornecedores cujos serviços adicionamos aos nossos portais e aplicativos. O usuário poderá proibir a execução destes cookies, mas algumas destas funcionalidades, ou mesmo todas, poderão não atuar como designado.
PUBLICIDADE	Cookies que podem ser estabelecidos em portais e aplicativos do ChildFund Brasil através de nossos parceiros de marketing. Serão utilizados por esses parceiros para construir um perfil e exibir conteúdo mais relevante ao interesse do usuário, assim como medir a eficácia de campanhas publicitárias. Não armazenam diretamente informações pessoais, mas são baseados na identificação exclusiva do seu navegador e dispositivo utilizado para acesso. O usuário poderá proibir a execução destes cookies, mas receberá menos publicidade direcionada.
REDES SOCIAIS	Cookies estabelecidos por terceiros e adicionados aos portais e aplicativos do ChildFund Brasil para acompanhamento de usuários de redes sociais que visitam nossas páginas, permitir o compartilhamento de nosso conteúdo com sua lista de amigos e conhecidos. Também são capazes de rastrear a sua navegação por outros websites e criar um perfil sobre os seus interesses. Isso pode afetar o conteúdo e as mensagens que vê nos outros websites que visita. Se não permitir estes cookies, talvez não consiga usar ou ver essas ferramentas de partilha.

A qualquer momento o usuário poderá revogar a sua autorização quanto à utilização dos cookies, acessando, para tanto, as configurações de seu navegador de preferência. Contudo, alertamos que, de acordo com as configurações executadas, certas funcionalidades dos nossos serviços poderão não funcionar da maneira ideal, bem como aspectos de segurança da informação.

12. SOBRE E-MAIL MARKETING

Ao se cadastrar para receber o e-mail marketing do ChildFund Brasil, o usuário declara concordar que o ChildFund Brasil realize uma compilação personalizada de notícias e ofertas, bem como avalie padrões de uso das plataformas, para o envio de comunicação personalizada que atenda às necessidades e interesses do usuário.

Caso o usuário deseje interromper o recebimento deste tipo de comunicação, poderá cancelar o cadastro a qualquer momento. Para isso, o usuário poderá clicar no link de *opt-out* presente nos e-mails recebidos para ser encaminhado ao processo de cancelamento ou poderá utilizar um dos meios de comunicação mencionados na presente Política de Privacidade.

13. LEI APLICÁVEL E DISPOSIÇÕES GERAIS

Este documento foi elaborado com base na regulamentação aplicável sobre segurança da informação, privacidade e proteção de dados, inclusive (sempre e

quando aplicáveis) a Constituição da República Federativa do Brasil, o Código de Defesa do Consumidor, o Código Civil, o Marco Civil da Internet (Lei Federal n. 12.965/2014), seu decreto regulamentador (Decreto 8.771/2016), a Lei Geral de Proteção de Dados Pessoais (Lei Federal n. 13.709/2018), e demais normas setoriais ou gerais sobre o tema.

Esta política está vinculada ao Termos de Uso, disponíveis no portal de privacidade ou no aviso de privacidade, e será interpretada segundo a legislação brasileira, no idioma português, sendo eleito o Foro Central da Comarca de Belo Horizonte para dirimir qualquer litígio, questão ou dúvida superveniente, com expressa renúncia de qualquer outro, por mais privilegiado que seja.

Caso alguma disposição desta Política de Privacidade seja considerada ilegal ou ilegítima por autoridade pública, as demais condições permanecerão em pleno vigor e efeito.

O usuário reconhece que toda comunicação realizada por e-mail (aos endereços por ele informados), SMS, aplicativos de comunicação instantânea ou qualquer outra forma digital e virtual também são válidas como prova documental, sendo eficazes e suficientes para a divulgação de qualquer assunto que se refere aos serviços prestados pelo ChildFund Brasil, bem como às condições de sua prestação, ressalvadas as disposições expressamente diversas previstas nesta Política de Privacidade.

14. FALE CONOSCO

Caso o titular deseje esclarecer alguma dúvida adicional, pedimos a gentileza de nos contatar através dos canais de relacionamento disponíveis no portal de privacidade ou no aviso de privacidade ou, caso prefira, diretamente junto ao encarregado de dados através do email privacidade@childfundbrasil.org.br.

15. ATUALIZAÇÕES DESTA POLÍTICA

A Política de Privacidade do ChildFund Brasil, disponibilizada nos canais mencionados no portal de privacidade ou no aviso de privacidade, é a versão mais atualizada do documento. O ChildFund Brasil pode, entretanto, a qualquer tempo e a seu exclusivo critério, atualizar a Política visando aprimorar a segurança, melhorar nossos serviços ou para atendimento de obrigações legais, regulatórias ou administrativas.

O ChildFund Brasil encoraja o titular a revisar periodicamente esta Política de Privacidade para se manter atualizado sobre como seus dados estão sendo tratados.

Se o usuário não aceitar e não concordar com esta Política de Privacidade, incluindo quaisquer alterações, não deverá acessar ou usar as plataformas, serviços e produtos do ChildFund Brasil.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO CHILDFUND BRASIL

OBJETIVO

Estabelecer os princípios e diretrizes para garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações lógicas e físicas processadas pelo ChildFund Brasil ("organização social sem fins lucrativos"), em todos os níveis da organização, respeitando a legislação e regulamentação vigentes sobre o tema.

DEFINIÇÕES

- Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- Autenticidade: garantia de identificação e registro do usuário que está produzindo, enviando ou modificando a informação, de forma claramente documentada.
- Confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas a terem acesso.
- Dado Anonimizado: dado pessoal relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável, desde que coletada em território nacional.
- 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.
- Diretriz: conjunto de instruções ou indicações para se tratar e levar a termo um plano, uma ação, um negócio.
- Disponibilidade: garantia de que usuários autorizados obtenham acesso à informação e aos ativos correspondentes.
- Incidente / Violação de Segurança: tentativa ou concretização de um evento que comprometa a integridade, autenticidade, conformidade ou disponibilidade de qualquer ativo da organização.

- Informação: recurso fundamental para o desenvolvimento das atividades do **ChildFund Brasil**, e, como tal, necessita ser protegida. A segurança da informação visa preservar a confidencialidade, integridade e disponibilidade da informação.

- Integridade: manutenção da informação na forma em que foram originalmente produzidas e armazenadas, não podendo sofrer modificações não autorizadas previamente. Tais modificações, quando não planejadas, podem gerar informações incorretas e comprometer a integridade de todo o sistema de informações.

- Plano de Contingência: também denominado de planejamento de riscos, plano de continuidade de negócios ou plano de recuperação de desastres, tem o objetivo de descrever as medidas a serem tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou em um estado minimamente aceitável, o mais rápido possível, evitando assim uma paralisação prolongada que possa gerar maiores prejuízos à organização.

- Proteção de Dados: ações integradas com o objetivo de promover a proteção dos dados pessoais, buscando sempre a sua anonimização, bem como a observância da legislação vigente.

- Segurança da Informação: proteção de um conjunto de informações no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas corporativos, informações eletrônicas ou sistemas de armazenamento. O conceito se aplica a todos os aspectos de proteção de informações e dados.

- Sigilo empresarial: proteção dos dados e documentos produzidos por uma empresa/organização no exercício de sua atividade econômica, buscando proteger as informações que propiciam ao ChildFund **Brasil** vantagens competitivas fundamentais para o êxito da atividade. Estão enquadradas nesta categoria marcas, patentes, know-how, análises e segredos.

PRINCÍPIOS

1.1 O ChildFund Brasil, para proteger as suas informações, visando a redução dos riscos de falhas, danos e/ou os prejuízos que possam comprometer a imagem e a continuidade dos objetivos da instituição, estabelece esta Política de Segurança da Informação. A Política de Segurança da Informação estabelece as diretrizes para a adoção de procedimentos e mecanismos relacionados à segurança da informação, de acordo com a legislação e regulamentação aplicável, bem como as diversas NORMAS NBR ISO/IEC existentes, devendo ser cumprida por todos os seus Empregados, colaboradores, visitantes, e prestadores de serviços terceirizados.

1.2 A informação é um ativo que possui grande valor, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, Internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc. Por princípio, a segurança da informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças, devendo abranger três aspectos básicos:

1.2.1 Confidencialidade: somente pessoas devidamente autorizadas pela organização devem ter acesso à informação;

1.2.2 Integridade: somente alterações, supressões e adições autorizadas pela organização devem ser realizadas nas informações;

1.2.3 Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

1.3 Os equipamentos e sistemas que viabilizam a atividade de acesso eletrônico à rede corporativa e à conexão com a Internet, assim como as informações geradas, recebidas, armazenadas e transmitidas compõem patrimônio da organização e, como tal, devem ser entendidos e protegidos.

ABRANGÊNCIA

1.1 Esta Política aplica-se ao ChildFund Brasil em toda a sua estrutura organizacional, ou seja, alta administração, gestores, funcionários, colaboradores, partes relacionadas, bem como prestadores de serviços, consultores, auditores, temporários, fornecedores, parceiros diversos e demais contratados que estejam a serviço do ChildFund Brasil.

1.2 A presente Política Normativa aplica-se a todos os setores que, de alguma forma, manuseiam dados e informações no ambiente do ChildFund Brasil.

DIRETRIZES E RESPONSABILIDADES RELACIONADAS

1.1 A Política de Segurança da Informação estabelece responsabilidades da instituição, gestores, empregados, colaboradores, visitantes e prestadores de serviços terceirizados.

1.2 O ChildFund Brasil assume o compromisso de utilizar informações confiáveis e íntegras, devendo:

1.2.1 Preservar a informação, confidencialidade, integridade e disponibilidade: Garantindo que as informações sejam acessadas somente pelas pessoas devidamente autorizadas a qualquer momento, com a sua exatidão e integridade, em conformidade com regimentos, regulamentos e a legislação pertinente.

1.2.2 Preservar e prevenir contra o uso indevido dos recursos de tecnologia da informação: Garantindo que os recursos computacionais e de comunicação sejam utilizados somente para a finalidade da organização.

1.3 O cumprimento das diretrizes deverá ser atingido através de:

1.3.1 Implementação da gestão da continuidade das atividades da organização: Assegurar a continuidade dos processos vitais à Organização, por meio da combinação de ação de prevenção e recuperação. Considerar prazos máximos de recuperação de sistemas de acordo com a criticidade dos processos.

1.3.2 Informações organizacionais: Garantir a proteção das informações da Organização contra perda, destruição ou falsificação, de maneira a atender os requisitos regulamentares e de auditoria.

1.3.3 Controle e gerenciamento da rede: Garantir a segurança dos dados da rede, assim como a proteção dos serviços oferecidos contra acessos não autorizados, utilizando um conjunto de controles, considerando o uso de tecnologias que assegurem a confidencialidade, integridade e disponibilidade dos dados que trafegam por redes públicas e privadas e coordenando as atividades de gerenciamento de forma a aperfeiçoar o serviço prestado para garantir a aplicação dos procedimentos de segurança em toda a infraestrutura de processamento da informação.

1.3.4 Monitoramento do uso e acesso ao sistema: Adotar sistemas de monitoramento com a finalidade de detectar divergências entre os eventos monitorados, fornecendo dessa maneira, evidências em caso de incidente de segurança da informação.

1.3.5 Respeito aos direitos de propriedade intelectual: Utilizar somente softwares adquiridos através de licenças, limitados à quantidade contratada, em respeito à legislação do direito autoral.

1.3.6 Registro de incidentes de segurança: Todos os incidentes de segurança relacionados à tecnologia da informação (fragilidades e ameaças, ocorridas ou suspeitas) devem ser notificados ao Setor de Tecnologia da Informação.

1.4 Todos os que ocupam alguma forma de acesso à rede interna obrigam-se ao cumprimento das seguintes diretrizes:

1.4.1 Utilizar os recursos de tecnologia da informação somente para a execução das atividades da organização quando necessário;

1.4.2 Racionalizar o envio e recepção de informações digitais, evitando excessos que sobrecarreguem a rede e provoquem lentidão na transmissão e recepção de informações e prejuízo para a organização;

1.4.3 Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela organização. Não divulgar informações privilegiadas da organização, sobre pena de sofrer as punições estabelecidas pela Instituição e previstas em Lei;

1.4.4 Não copiar ou distribuir os conteúdos e mídias disponibilizados nos repositórios da organização;

1.4.5 Realizar somente *download* de arquivos da Internet que sejam necessários ao desempenho de suas atividades, sendo esses homologados e licenciados;

1.4.6 Encerrar a sessão de trabalho do ativo ao término da utilização e desligar os equipamentos;

1.4.7 Não instalar equipamentos pessoais ou de terceiros no ambiente da organização, sem prévia autorização.

1.4.8 Utilizar dispositivos móveis ou portáteis particulares nas dependências da organização é de inteira responsabilidade do seu proprietário, tanto por conteúdos neles instalados ou armazenados, sejam softwares ou dados;

1.4.9 Conectar dispositivos móveis ou portáteis na rede da organização tornará passível de monitoramento.

1.5 As empresas e prestadores de serviços terceirizados obrigam-se ao cumprimento das seguintes diretrizes:

1.5.1 Estar ciente da presente Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;

1.5.2 Tornar-se responsável pelos equipamentos que utilizar ou instalar no ambiente da organização;

1.5.3 Formalizar a necessidade de utilizar áreas de acesso restrito ou equipamentos da organização, não especificadas em contrato, através de documento que conste a finalidade, os profissionais e o tempo de acesso.

VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1.1 As seguintes condutas serão classificadas como falta grave e o infrator estará sujeito a sanções administrativas, de acordo com as normas disciplinares da organização:

1.1.1 Utilizar os Recursos de Tecnologia da Informação (TI) para fins que não sejam relacionados às atividades da organização;

1.1.2 Utilizar os recursos de TI da organização para conseguir acesso não autorizado a qualquer outro computador, rede, banco de dados ou informação armazenada eletronicamente (interna ou externamente);

1.1.3 Divulgar informações confidenciais ou de propriedade da organização, sem a devida autorização;

1.1.4 Enviar em nome da organização, mensagens que externem opiniões pessoais;

1.1.5 Enviar mensagens com conteúdo sexual, político, ideológico, racista, discriminatório, ofensivo ou difamatório ou que comprometam a reputação ou imagem da organização;

1.1.6 Acessar ou armazenar material pornográfico, jogos, chats, redes sociais, e-mail particular ou softwares de descentralização das funções convencionais de rede;

1.1.7 Copiar, distribuir ou imprimir material protegido por direitos autorais, sem permissão;

1.1.8 Desativar ou violar os dispositivos de segurança instalados nos equipamentos;

1.1.9 Retirar do local os equipamentos de TI sem a autorização do setor de TI.

MONITORAMENTO

1.1 O monitoramento da utilização dos recursos de TI é direito da organização, amparado legalmente, e como tal, é suscetível aos processos de auditoria. Compete ao Setor de TI da organização monitorar, a qualquer tempo e sem prévio aviso, todos os acessos a qualquer computador na Internet, bem como o envio e recepção de mensagens e utilização de softwares com o intuito de assegurar que os recursos computacionais e de comunicação oferecidos pela organização sejam utilizados somente para as atividades da qual a organização se propõe.

NORMAS DE UTILIZAÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA

1.1 Ao utilizar da estrutura de informática da organização, todos os usuários automaticamente aceitam seu conjunto de regras e no caso do não cumprimento de alguma norma, estarão sujeitos às advertências verbais ou escritas e suspensão do uso deste acesso por prazo a ser determinado pelo Comitê de Segurança da Informação.

1.2 A Estrutura de Informática da **organização** é destinada, prioritariamente, ao desenvolvimento de atividades organizacionais a todos os empregados e para o uso da Internet como forma de maximizar o acesso à informação, trabalhos empresariais e desenvolvimento de suas atividades pertinentes à sua função.

1.3 Os microcomputadores, programas e o acesso à Internet pelos usuários, objetivam:

1.3.1 A segurança da estrutura de informática da **organização** e, também, dos seus usuários, todos os acessos e atividades realizadas serão monitorados.

1.3.2 O Departamento de Tecnologia da Informação terá o direito de vistoriar arquivos dos usuários da rede e dos ativos concedidos sob sua responsabilidade de administração, a fim de manter a segurança destes usuários e a integridade do sistema. Esta vistoria será feita, a qualquer momento, pelo setor de Tecnologia da Informação ou sempre que solicitado pelo superior direto, de forma a garantir a integridade dos dados neles contidos;

1.3.3 O Departamento de Tecnologia da Informação, não se responsabiliza por eventuais perdas de dados ou danos causados aos usuários por *hackers*, vírus de

computador ou por quaisquer problemas na rede provocados pelo descumprimento das normas da política de segurança da informação pelo respectivo usuário.

1.3.4 A **organização**, através do Departamento de Tecnologia da Informação, se reserva no direito de remover softwares sem prévio aviso ao usuário, desde que o conteúdo burle alguma das restrições apresentadas neste documento.

1.3.5 É proibido copiar programas instalados nos microcomputadores.

1.3.6 As páginas e programas considerados de conteúdo não pertinente à área empresarial serão bloqueados pela equipe de tecnologia da informação a qualquer momento sem aviso prévio.

1.3.7 Para utilização da estrutura é necessário o fornecimento de uma conta de acesso. A abertura desta conta é solicitada pelo responsável após a contratação do funcionário pela **organização**.

1.3.8 A **organização**, através de seu Departamento de Tecnologia da Informação, reserva-se o direito de suspender contas de usuários para manter a segurança e a integridade do sistema, pelo não cumprimento das normas aqui estabelecidas ou desligamento do quadro funcional.

1.3.9 É considerado usuário qualquer pessoa autorizada (funcionário, colaborador, visitante, terceirizado) que utiliza de alguma forma recurso computacional da **organização**.

1.3.10 Para utilização dos recursos de informática em situações extraordinárias, os usuários devem formalizar solicitação por escrito ao Departamento de Tecnologia da Informação, com antecedência, para as providências institucionais;

1.3.11 Os administradores e o setor de TI têm o direito de não permitir a utilização da rede interna ou utilização de equipamentos de informática da **organização** a pessoas estranhas;

1.3.12 A permissão de acesso a terceiros deve ser feita por escrito e autorizada por algum Gerente/Diretor.

NORMAS DE UTILIZAÇÃO DE SOFTWARE (PROGRAMAS)

1.1 A organização disponibiliza aos seus usuários um conjunto de softwares exclusivamente para o desempenho de suas atividades e suas funções administrativas. É vedada ao usuário a instalação e execução de qualquer software, sem autorização prévia do Setor de TI. Todos os softwares instalados e executados nos computadores da organização devem ser devidamente licenciados, e o uso de qualquer software que não seja autorizado e/ou que viole os direitos do autor do programa são terminantemente proibidos.

NORMAS DE UTILIZAÇÃO DA REDE

1.1 Não são permitidas tentativas de obter acesso não autorizado, tais como, tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário, ou colocar à prova a segurança de outras redes.

1.2 Não são permitidas alterações das configurações de rede e inicialização dos computadores, bem como, modificações que possam trazer algum problema futuro.

1.3 Material sexualmente explícito não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede corporativa.

1.4 Todos os arquivos devem ser gravados na rede, pois arquivos gravados no computador (local) não possuem cópias de segurança (backup) e podem ser perdidos. O espaço em disco é controlado por departamento, por isso, os usuários devem administrar seus arquivos gravados, excluindo os arquivos desnecessários. Importante citar que não é responsabilidade da área de TI a recuperação de arquivos que não respeitem a regra acima citada.

1.5 Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos, etc.) nos drivers de rede, pois ocupam espaço comum limitado do departamento.

ACESSO A INTERNET

1.1 A Internet é uma ferramenta de trabalho que deve ser utilizada para esse fim pelos usuários da organização. Não é permitido o seu uso para fins pessoais ou recreativos em horários de trabalho. É proibida a divulgação de informações confidenciais da organização, sendo passível sofrer as penalidades previstas na forma da Lei.

1.2 O envio e recepção de informações digitais devem ser racionalizados, evitando excessos que sobrecarregam a rede e provocam lentidão na transmissão e recepção de informações e prejuízo para a organização.

1.3 Os downloads de arquivos da Internet devem ser realizados através de sites confiáveis e somente os que sejam necessários ao desempenho das atividades. Poderão ser bloqueados arquivos e/ou domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos. Todo acesso dos usuários a sites será armazenado na forma de log, possibilitando auditorias futuras. Não é permitido burlar a estrutura de TI da organização.

NORMAS DO USO DE IMPRESSORAS

1.1 Documento enviado para a impressão deverá ser retirado imediatamente. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável e com senha. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não-autorizado. Isto é, documentos esquecidos nas impressoras, ou com demora para retirada, ou até mesmo em cima da mesa, podem ser lidos, copiados ou levados por outro funcionário ou por alguém de fora da organização.

1.2 O uso das impressoras deve ser feito exclusivamente para impressão de documentos ou outras informações que sejam de interesse da organização ou que estejam relacionados com o desempenho de suas atividades.

VERIFICAÇÃO DA UTILIZAÇÃO DA POLÍTICA

1.1 Para garantir o cumprimento das normas mencionadas acima, o ChildFund Brasil se reserva no direito de:

1.1.1 Implantar sistemas que possibilitem monitorar e gravar todos os acessos à Internet, software e computadores da organização.

1.1.2 Auditar qualquer arquivo armazenado na rede, tanto no disco local do computador ou nas áreas privadas da rede, visando assegurar o cumprimento desta política.

COMPETÊNCIAS E RESPONSABILIDADES

1.1 As competências e responsabilidades dos entes que compõem a estrutura de segurança da informação do **ChildFund Brasil** estão previstas no Estatuto Social, Regimento Interno e normativos da **organização**.

1.2 Juntamente com a Política de Segurança da Informação fica instituído o Comitê de Segurança da Informação, sendo o responsável pela implementação e cumprimento da presente Política.

1.2.1 O Comitê de Segurança da Informação é composto pelos ocupantes dos seguintes cargos do **ChildFund Brasil**:

- Responsável pela Diretoria de País;
- Responsável pelo RH;
- Responsável pela área de Proteção de Dados;
- Responsável pela área de TI;
- Responsável pelo Jurídico e Administrativo;
- Responsável por Finanças e Contabilidade;
- Responsável por Programas e Apadrinhamento;
- Responsável por Mobilização de Recursos e Desenvolvimento de Novos Negócios.

1.3 O Setor de TI e o Comitê de Segurança da Informação serão os responsáveis por implementar as regras definidas nesta Política, sendo responsáveis, também, pela adoção de medidas técnicas adicionais necessárias à manutenção da infraestrutura e à otimização do uso dos recursos de tecnologia da informação. O Setor de TI poderá, a qualquer momento, verificar os computadores, com o objetivo de averiguar e identificar possíveis não conformidades descritas nesta Política de Segurança da Informação.

1.4 Ademais, todos os usuários da organização devem seguir as Normas de Segurança Interna para a Utilização dos Recursos de TI, visando o adequado emprego de seus recursos.

DISPOSIÇÕES FINAIS

1.1. Esta política será revisada anualmente e, caso necessário, em período inferior à exclusivo critério da organização.

1.2. O ato de aprovação digitalizada da presente política, em formato de documento PDF, está arquivado na rede do ChildFund Brasil.

1.4 As dúvidas de interpretação desta Política, bem como os casos omissos, serão dirimidos pelo Comitê de Segurança da Informação.

1.5 A presente política passa a vigorar a partir da data de sua aprovação, sendo válida por tempo indeterminado.

CONTATO

Se tiver alguma dúvida, comentário ou sugestão, por favor, entre em contato com a nossa Encarregada pelo Tratamento de Dados Pessoais (“Data Protection Officer”), Sra. Joyce Mara a qual pode ser contatada através do e-mail privacidade@childfundbrasil.org.br.