ORDEM DE SERVIÇO DTI Nº 005/2023

Dispõe sobre a política de governança e proteção de dados no âmbito da Fundação CASA/SP – Centro de Atendimento Socioeducativo ao Adolescente do Estado de São Paulo.

A **Divisão de Tecnologia da Informação (DTI),** no uso das atribuições conferidas a este departamento, junto com suas gerências e seções, resolvem:

Artigo 1º - As regras e diretrizes aqui estabelecidas devem ser seguidas por todos os **USUÁRIOs,** sem quaisquer exceções.

Artigo 2º - Esta **OS** se aplica aos dados que identificam o **USUÁRIO** individualmente **(dados pessoais)** e demais dados fornecidos por ele ou coletados durante a utilização dos sites e sistemas web da **Fundação CASA/SP.** Em todos os casos, a instituição cumpre com toda legislação brasileira aplicável à proteção de dados.

CAPÍTULO I - FUNDAMENTAÇÃO LEGAL E NORMATIVA

Artigo 3º - A presente **OS** está fundamentada nos seguintes instrumentos legais e normativos:

I. Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991, e dá outras providências;
II. Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
III. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição;
IV. Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco civil da Internet;
V. Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados (LGPD);
VI. Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril (“GDPR”);
VII. DN CGGDIESP-1, de 30 de dezembro de 2021, que traz boas práticas em segurança da informação, para privacidade e proteção de dados pessoais e para a gestão de dados e informações;
VIII. DO SP V132/N259, de 29 de dezembro de 2022; IN PGDI-1, de 27 de dezembro de 2022, referente ao anexo II, 3 - Tabela de Providências Complementares e Responsáveis - Ativos da Informação: Orientação Técnica e Modelo - Inventário de Dados, da Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021;
IX. Ordens de Serviço publicadas pela Divisão de Tecnologia da Informação (Fundação CASA/SP).

CAPÍTULO II - CONCEITOS E DEFINIÇÕES

Artigo 4º - Para fins desta **OS,** considera-se que:

I. **OS:** Ordem de Serviço;

II. **Divisão de Tecnologia da Informação (DTI):** departamento com a responsabilidade de dispor, gerir e implementar todas as ações de gestão e segurança da informação e comunicações no âmbito institucional;

III. **TIC:** tecnologia da informação e comunicação;

IV. **site/website:** é uma coleção de páginas da web organizadas e localizadas em um servidor na rede. Imagine um site como uma casa onde você reúne seus móveis (as informações dele) em cômodos (as páginas dele). Um website pode tratar de diversos assuntos e disponibilizam as informações em forma de conteúdo de texto e mídia;

V. **aplicação/sistema web:** é um website com a adesão de novas tecnologias, sendo agora capaz de manipular e armazenar determinados tipos de dados. Também é composto por diversas páginas e além delas possui um banco de dados próprio;

VI. **dado(s) pessoal(ais):** qualquer informação que, direta ou indiretamente, sozinha ou acompanhada de outros dados, identifique ou possa identificar uma pessoa física. São exemplos de dados pessoais: nome, CPF, número de Protocolo de Internet (IP), endereço de e-mail, número de conta bancária, perfil financeiro, identificação de contribuinte, registro profissional, geolocalização, dentre outros. Incluem-se neste conceito os **dados pessoais sensíveis,** conforme definição abaixo;

VII. **dado(s) pessoal(ais) sensível:** um 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;

   i. **Quando houver tratamento GDPR:** significa qualquer **dado pessoal** que revele a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.

VIII. **dado(s) anonimizado(s):** o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

   i. **Quando houver tratamento GDPR:** significa o dado relativo a um titular que não pode ser identificado após a aplicação de técnicas de anonimização. A anonimização é uma técnica que resulta do **tratamento de dados pessoais** a fim de lhes retirar elementos suficientes para que deixe de ser possível identificar o Titular, de forma irreversível;

IX. **dado pessoal pseudoanonimizado:** um tipo de **dado pessoal** tratado de forma a não ser mais relacionável a uma pessoa específica sem que seja necessário recorrer a informações suplementares, desde que tais informações sejam mantidas separadamente e estejam sujeitas a medidas técnicas e organizacionais que assegurem que os **dados pessoais** não possam ser atribuídos a uma pessoa identificada ou identificável;

X. **titular(es):** qualquer pessoa física identificada ou que possa ser identificada pelo **tratamento dos dados pessoais** ou **dados pessoais sensíveis;**

XI. **tratamento:** toda e qualquer operação realizada com os **dados pessoais** ou **dados pessoais sensíveis,** incluindo, mas não se limitando, 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;

XII. **violação de dados pessoais:** toda e qualquer situação, acidental ou intencional, praticada mediante culpa ou dolo, que provoque, em relação a Dados Pessoais: (i) a destruição; (ii) a perda; (iii) a alteração; (iv) a comunicação, difusão ou divulgação; ou (v) o acesso não autorizado;

XIII. **controladora** ou ***controller*** ou **responsável pelo tratamento:** a parte a quem compete as decisões relativas ao **tratamento de dados pessoais;**

XIV. **operadora** ou ***processor*** ou **subcontratante:** a parte que realiza o **tratamento de dados pessoais** em nome e sob as instruções da **controladora;**

XV. **controladora(s) conjunta(s):** quando as partes em conjunto têm a competência de decidir sobre o **tratamento de dados pessoais;**

XVI. **relatório de impacto à proteção de dados pessoais (RIPD)** ou ***data protection impact assessment*** **(DPIA):** a documentação da **controladora** que contém a descrição e avaliação dos processos de **tratamento de dados pessoais,** seus eventuais riscos e impactos às liberdades civis e aos direitos fundamentais dos **titulares,** bem como medidas, salvaguardas e mecanismos de mitigação de risco;

XVII. **encarregado** ou ***data protection officer*** **(DPO):** pessoa indicada pela presidência da **Fundação CASA/SP** para atuar como canal de comunicação entre o **órgão,** os **titulares dos dados pessoais,** a **Autoridade Nacional de Proteção de Dados (ANPD)** e, se houver necessidade, a autoridade pública independente criada por um Estado-Membro da União Europeia com a responsabilidade pela fiscalização da aplicação do **GDPR,** bem como as demais responsabilidades estabelecidas no **Artigo 13;**

XVIII. **ciclo de vida do dado pessoal:** representa todos os fluxos de **tratamento** aos quais o **dado pessoal** é submetido durante sua existência nos sistemas e bases de dados da instituição;

XIX. **transferência internacional de dados pessoais:** significa a transferência de **dados pessoais** para país estrangeiro ou organismo internacional;

XX. **transferência internacional de dados pessoais para fins de GDPR:** significa a transferência de **dados pessoais** de um país da União Europeia para um país terceiro (não localizado na União Europeia) ou uma organização internacional, podendo a transferência ocorrer entre dois ou mais responsáveis pelo tratamento, responsáveis pelo tratamento e subcontratantes ou simplesmente ser alojados num espaço virtual fora da União Europeia sem que os **dados pessoais** sejam transferidos para outra pessoa física ou jurídica;

XXI. **terceiro:** pessoa física ou jurídica, autoridade pública, serviço ou organismo que seja prestador de serviço, parceiro, cliente, fornecedor ou qualquer outro terceiro;

XXII. **autoridade competente:** significa a **Autoridade Nacional de Proteção de Dados (ANPD)** e a autoridade pública independente criada por um Estado-Membro da União Europeia com a responsabilidade pela fiscalização da aplicação do **GDPR;**

XXIII. **representante:** uma pessoa física ou jurídica estabelecida na União Europeia que, designada por escrito pelo responsável pelo tratamento ou subcontratante que tenha o seu estabelecimento fora da União Europeia, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do **GDPR;**

XXIV. **acesso:** ato ou permissão para ingressar, transitar, conhecer, consultar, manipular e utilizar os ativos de informação;

XXV. **controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;

XXVI. **administradores de TIC:** são as pessoas designadas formalmente, pela autoridade máxima da **DTI,** com atribuição principal de ser o responsável técnico pelos seus recursos de **TIC;**

XXVII. **USUÁRIO:** é qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a **Fundação CASA/SP,** ou em condição autorizada, que utiliza, de qualquer forma, algum recurso de **TIC** da instituição.

CAPÍTULO III – OBJETIVO

Artigo 5º - A **DTI** e toda a **Fundação CASA/SP** estão comprometidas em manter sempre as melhores práticas no que diz respeito a questões de **proteção de dados pessoais** que são tratados em seus ambientes.

Artigo 6º - Esta **OS** tem por objetivo apresentar os princípios e as diretrizes que norteiam as atividades de **tratamento de dados pessoais** realizadas pela instituição.

Artigo 7º - Política, para os casos a seguir, denominados de **tratamentos GDPR:**

I. o **tratamento de dados pessoais** incidir sobre **titulares** localizados na União Europeia quando pretenda monitorar o seu perfil comportamental e o comportamento submetido ao mencionado monitoramento ocorra na União Europeia.

CAPÍTULO IV – PRINCÍPIOS NORTEADORES

Artigo 8º - A **DTI** e a **Fundação CASA/SP** ao realizarem quaisquer atividades de **tratamento de dados pessoais** devem observar os seguintes princípios:

I. Finalidade, licitude e lealdade;
II. Adequação e limitação das finalidades;
III. Necessidade;
IV. Livre acesso;
V. Transparência;
VI. Segurança, Prevenção, Integridade e Confidencialidade;
VII. Não discriminação;
VIII. Prestação de Contas, Responsabilidade *(accountabilty);*
IX. Exatidão; e
X. Limitação da conservação.

CAPÍTULO V – DIRETRIZES

Artigo 9º - Deve ser mantido controle direto dos **dados pessoais** que são tratados no escopo de seus serviços. Os processos de negócio, sistemas de suporte e relacionamento devem ser desenvolvidos com o mais elevado grau de segurança dos **dados pessoais** e aderência a legislação e normativos que regem o tema.

Artigo 10 - Os fluxos de **tratamento de dados pessoais** realizados pela **DTI** e **Fundação CASA/SP** devem ser devidamente mapeados e enquadrados em uma das bases legais previstas na legislação aplicável, mantendo o registro de atividades de **tratamento de dados pessoais** completo.

Artigo 11 - Ademais, o **órgão** deve observar as seguintes diretrizes, para garantia da governança de proteção de **dados pessoais.**

§ 1º - gestão de terceiros: procedimentos e regras contratuais em relação aos **terceiros** envolvidos nas suas atividades de **tratamento de dados pessoais,** de modo que estes fiquem obrigados a adotar medidas técnicas e organizacionais com vistas a Proteção dos Dados Pessoais nos termos desta **OS** e demais leis aplicáveis;

§ 2º - relatórios de impacto a proteção de dados pessoais (RIPD) ou ***data protection impact assessments*** **(DPIA):** elaboração e registro de **DPIAs** dos **tratamentos de dados pessoais** quando assim for necessário para atender à legislação aplicável ou à solicitação de **autoridade competente,** procurando identificar as medidas necessárias para eliminar ou mitigar os altos riscos aos direitos dos **titulares;**

§ 3º - **direitos dos titulares:** exercício, pelos **titulares** ou por representante legal, mediante uso dos canais disponíveis de atendimento institucional;

§ 4º - transferências internacionais: realizadas de acordo com as hipóteses autorizativas previstas na legislação aplicável;

§ 5º - privacidade e segurança por design e por padrão ou ***privacy and security by design and by default:*** os serviços e produtos devem, desde sua concepção, ter como padrão a observância dos princípios gerais de proteção de **dados pessoais** e privacidade, bem como medidas de **segurança da informação;**

§ 6º - gestão de incidentes de violação de dados pessoais: estabelecimento de um **plano de incidentes de violação de dados pessoais** para adoção das providências adequadas conforme a legislação aplicável.

CAPÍTULO VI – DIRETRIZES PARA OS TRATAMENTOS GDPR

Artigo 12 - Na observância dos **CAPÍTULOS IV** e **V** estabelecidos nesta **OS,** devem ser considerados também os conceitos definidos no item **Artigo 3º** desta, indicados de forma específica.

CAPÍTULO VII – RESPONSABILIDADES

Artigo 13 - Do **encarregado de proteção de dados pessoais:**

I. Gerir os processos e os procedimentos de **proteção de dados pessoais;**
II. Atuar como ponto focal do **órgão** em assuntos relacionados à **proteção de dados pessoais;**
III. Receber e realizar comunicações de qualquer autoridade fiscalizadora nacional ou internacional, incluindo, mas não se limitando, à **ANPD,** às autoridades nacionais de proteção de dados da União Europeia, dentre outras;
IV. Garantir a observância aos direitos dos **titulares** de **dados pessoais;** e
V. Promover a conscientização e educação sobre **proteção de dados pessoais.**

Artigo 14 - Da **área de proteção de dados.**

I. Apoiar o **encarregado** na execução de suas responsabilidades.

Artigo 15 - Dos **proprietários da informação.**

I. Os **proprietários de informações,** que tratem **dados pessoais** e/ou **dados pessoais sensíveis,** deverão levar em consideração as diretrizes desta **OS** e da **OS** sobre **Política de Identidade e Controle de Acesso,** nas atividades de classificação, proteção, controle e autorização de acesso à Informação.

CAPÍTULO VIII – DISPOSIÇÕES FINAIS

Artigo 16 - A **DTI** pode alterar o teor desta **OS** a qualquer momento, conforme a finalidade ou necessidade, tal qual para adequação e conformidade legal de disposição de lei ou norma que tenha força jurídica equivalente, cabendo ao **USUÁRIO** verificá-la.

§ 1º - Ocorrendo atualizações significativas neste documento e que demandem coleta de consentimento, a instituição notificará o **USUÁRIO** pelo e-mail fornecido e canais de atendimento.

Artigo 17 - Caso haja alguma dúvida sobre as condições estabelecidas nesta **OS** ou qualquer documento, o **USUÁRIO** pode entrar em contato por meio dos canais de atendimento supramencionados.

Artigo 18 - Caso alguma disposição desta **OS** seja considerada ilegal ou ilegítima por autoridade da localidade em que o **USUÁRIO** resida ou da sua conexão à rede local e Internet, as demais condições permanecerão em pleno vigor e efeito.

Artigo 19 - 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, virtual e digital também são válidas como prova documental, sendo eficazes e suficientes para a divulgação de qualquer assunto que se refira aos serviços prestados pela **Fundação CASA/SP,** bem como às condições de sua prestação, ressalvadas as disposições expressamente diversas previstas nesta **OS.**

Artigo 20 - Esta **OS** e a relação decorrente das ações aqui compreendidas, assim como qualquer disputa que surja em virtude disto será regulada exclusivamente pela legislação brasileira.

Artigo 21 - Fica eleita a **Assessoria Jurídica (AJ)** da **Fundação CASA/SP** para dirimir qualquer questão envolvendo o presente documento, renunciando as partes a qualquer outro, por mais privilegiado que seja ou venha a ser.

Artigo 22 - Os casos de **não conformidade** serão avaliados pela **DTI** e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP.**

Artigo 23 - Esta **OS** entra em vigor na data de sua publicação.

CAPÍTULO IX – VERSIONAMENTO

VERSÃO	DATA	AUTOR	DESCRIÇÃO
1.0	29/12/2022	Julio Cesar Signorini	**Versão Inicial**
1.1	10/01/2023	Alex Christy Rogatti, Aurélio Olímpio de Souza, João Paulo Puntel Vargens, Julio Cesar Signorini, Luiz Fernando Souza Gomes da Silva, Marcelo Pereira da Silva, Márcia Ramos dos Santos, Odenilson dos Santos Bonfim, Patricia Tsutsumi Dias, Rafael Mengel Souza, Rodrigo Braoios Vilhora e Yuri Horalek e Domigues	**Revisões e Sugestões**
1.2	12/01/2023	AJ (Assessoria Jurídica), DGA (Diretoria de Gestão Administrativa), DTI (Divisão de Tecnologia da Informação) e GP (Gabinete da Presidência)	**Versão Final**

DTI, 12 de janeiro de 2023.

DOCUMENTO ASSINADO DIGITALMENTE