ORDEM DE SERVIÇO DTI Nº 001/2023

Dispõe sobre a política de gestão de identidade, métodos de autenticação de usuários e controle de acesso aos recursos de TIC 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.

CAPÍTULO I - FUNDAMENTAÇÃO LEGAL E NORMATIVA

Artigo 2º - 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 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, 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;

V. 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;

VI. 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;

VII. ABNT NBR ISO/IEC 27001:2013, que trata dos sistemas de gestão da segurança da informação – requisitos;

VIII. ABNT NBR ISO/IEC 27002:2013, que estabelece o código de prática para controles de segurança da informação;

IX. Ordens de Serviço publicadas pela Divisão de Tecnologia da Informação (Fundação CASA/SP).

CAPÍTULO II - CONCEITOS E DEFINIÇÕES

Artigo 3º - Para fins desta **OS,** considera-se que:

I. **OS:** Ordem de Serviço;
II. **Divisão de Tecnologia da Informação (DTI):** departamento com a responsabilidade de implementar todas as ações de segurança da informação e comunicações no âmbito institucional;
III. **TIC:** tecnologia da informação e comunicação;
IV. **ativo:** qualquer coisa que tenha valor para a **Fundação CASA/SP**;
V. **ativos de TIC:** são todos os itens, físicos ou virtuais, que compõem a infraestrutura de **TIC** da instituição. Ou seja, tudo que é hardware, software, redes e outras tecnologias fundamentais para a continuidade das operações de quase todo tipo de negócio;
VI. **autenticação:** processo que busca verificar e confirmar a identidade do **USUÁRIO;**
VII. **confidencialidade:** propriedade da informação que garante que esta não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização;
VIII. **acesso:** ato ou permissão para ingressar, transitar, conhecer, consultar, manipular e utilizar os ativos de informação;
IX. **acesso privilegiado:** acesso a ambientes restritos ou controlados e informações sensíveis;
X. **acesso restrito:** acesso limitado ou controlado concedido sob condições específicas;
XI. **análise de riscos:** conjunto de procedimentos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, mediante o equilíbrio dos custos operacionais e financeiros envolvidos;
XII. **classificação da informação:** atribuição pela autoridade competente do grau de sigilo dado à informação, documento, material, área ou instalação;
XIII. **controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;
XIV. **gestão de segurança da informação e comunicação:** ações e métodos que visam a integração das atividades de análise de riscos, gestão de continuidade do negócio, tratamento de incidentes, classificação e tratamento da informação, conformidade, credenciamento, segurança cibernética, física, lógica, de recursos humanos e documental aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à **TIC;**
XV. **gestor de segurança da informação e comunicações:** pessoa responsável designada pela autoridade máxima da **DTI** pelas ações de segurança da informação e comunicações no âmbito da instituição;
XVI. **gestor de sistema:** gestor departamental e/ou servidor/colaborador da **Fundação CASA/SP** designado formalmente para gerenciar os acessos ao sistema de informação de sua área de negócio/departamento, sendo responsável pela autorização e remoção dos acessos;
XVII. **informações sensíveis:** ativos de informação que têm caráter privado ou possuem restrições quanto à sua publicação, cujo acesso indevido poderão gerar danos ou perdas pessoais e à instituição;
XVIII. **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;**

XIX. **representante de USUÁRIOs:** é o gestor imediato ou a pessoa designada formalmente de uma localidade/departamento, pela autoridade máxima da localidade/departamento, com a atribuição de representar seus **USUÁRIOs,** nos assuntos relacionados com a utilização dos recursos de **TIC** da **Fundação CASA/SP;**

XX. **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 - OBJETIVOS E DIRETRIZES

Artigo 4º - Constituem objetivos da presente **OS:**

I. garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação;

II. estabelecer mecanismos e controles para garantir a efetiva proteção dos dados, informações e conhecimentos gerados;

III. reduzir os riscos de ocorrência de perdas, alterações e acessos indevidos aos ativos de informação;

IV. preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações;

V. garantir o direito de acesso, considerando a classificação da informação produzida, as obrigações da legislação vigente e a análise de riscos existente;

VI. definir o nível de acesso baseado em normas internas e procedimentos formais específicos;

VII. revisar e controlar os acessos de forma periódica e manter o seu registro disponível para consulta individual ou de auditoria;

VIII. exigir procedimentos formais para o fornecimento de informações ou transferência de ativos físicos de áreas restritas para áreas de criticidade diferente de sua origem, segundo a classificação da informação e a análise de riscos existente; e

IX. elaborar normas internas ou procedimentos formais específicos para acessos por meio de dispositivos particulares que fizerem uso da infraestrutura da **Fundação CASA/SP.**

Artigo 5º - Constituem diretrizes da presente **OS:**

I. garantia de que os acessos aos ativos de informação sejam autorizados com base em níveis de restrições;

II. instituição de procedimentos prévios de credenciamento para a criação de contas de acesso e utilização de credenciais físicas para o acesso aos ativos de informação;

III. uso das credenciais de acesso de modo pessoal e intransferível, permitindo de maneira clara e inequívoca o reconhecimento do **USUÁRIO;**

IV. conscientização dos **USUÁRIOs** sobre a necessidade de sigilo, conforme classificação da informação e características de chaves de acesso;

V. registro dos acessos aos ativos de informação da **Fundação CASA/SP;**

VI. existência de responsáveis formais pela concessão e manutenção dos acessos privilegiados;

VII. observância da legislação específica para a concessão e controle de acesso às informações sensíveis ou sigilosas;

VIII. utilização de ferramentas ou protocolos de proteção contra acesso não autorizado aos ativos de informação;
IX. distinção de acesso para servidores e público em geral;
X. bloqueio ao acesso e apuração da responsabilidade administrativa, penal e civil do **USUÁRIO** pelo uso indevido ou acesso não autorizado aos ativos de informação;
XI. revisão do acesso concedido aos **USUÁRIOs** que tiveram mudança em suas atribuições, devendo ser readequados imediatamente ou bloqueados em caso de perda do vínculo com a Instituição;
XII. classificação dos ativos de informação de acordo com o valor, a criticidade, o tipo de ativo e o grau de sigilo das informações que podem ser tratadas em tais ativos, devendo ser mapeados aqueles considerados críticos;
XIII. difusão e exigência do cumprimento da presente Política e da legislação de regência do assunto;
XIV. identificação e avaliação sistemática dos riscos à segurança da informação e comunicações dos ativos de informação;
XV. definição de regras específicas para autorizar o acesso e o credenciamento dos **USUÁRIOs** em conformidade com a classificação dos ativos de informação;
XVI. concessão de acesso aos ativos de informação restrita ao exercício das atividades do cargo, função ou atribuições de cada **USUÁRIO;** e
XVII. responsabilização do **USUÁRIO** pelas ações realizadas por meio de sua credencial de acesso.

CAPÍTULO IV - CREDENCIAIS DE ACESSO

Artigo 6º - Os controles de acesso implementados na **Fundação CASA/SP** devem aplicar o princípio ***"necessidade de conhecer"*,** o qual prescreve a necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio ***"privilégio mínimo"*,** o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades.

Artigo 7º - Os controles de acesso lógicos na instituição devem utilizar, preferencialmente, autenticação com certificado digital **ICP-Brasil,** a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais.

Artigo 8º - A credencial de acesso é formada pelo nome de **USUÁRIO *(login)*** e uma senha de acesso.
§ 1º - O nome de **USUÁRIO *(login)*** deve seguir a padronização estabelecida pela **DTI.**

Artigo 9º - O **gerenciamento de senhas** constitui o mecanismo básico para a autenticação de **USUÁRIOs** em dispositivos de **TIC** e aplicações/sistemas computacionais da **Fundação CASA/SP,** podendo haver a adoção de outros tão ou mais seguros que este.

Artigo 10 - As senhas das contas pessoais são **confidenciais, intransferíveis** e é responsabilidade do **USUÁRIO** mantê-la como tal, observando mecanismos de segurança e integridade. São atribuídas a cada indivíduo como um mecanismo para controlar e monitorar seu acesso a aplicações e informações e não podem ser compartilhadas com outras pessoas.

Artigo 11 - As senhas das **contas institucionais** ficarão vinculadas à matrícula (RE) do funcionário/servidor indicado pela autoridade máxima da localidade/departamento, recaindo sobre este toda a responsabilidade pelo seu uso.

Artigo 12 - Novas senhas serão fornecidas e senhas já existentes serão liberadas apenas quando a identidade do requisitante estiver assegurada.

§ 1º - O **USUÁRIO** será responsabilizado pelas ações de outros se, desrespeitando o **Artigo 10º,** deliberadamente, compartilhar sua senha e/ou acesso;

§ 2º - Em caso de suspeita de violação, o **USUÁRIO** deve avisar imediatamente ao **Service Desk** da **DTI** e trocar/alterar as senhas celeremente;

§ 3º - As senhas devem possuir no mínimo **8 (oito) caracteres** e conter ao menos **3 (três)** das **4 (quatro) diretrizes** abaixo:

I. Conter pelo menos uma letra maiúscula;
II. Conter pelo menos uma letra minúscula;
III. Conter números (0 a 9);
IV. Conter símbolos, incluindo: ! @ # $ % ^ & * - _ + = [ ] { } | \ : ‘ , . ? / ` ~ “ < > ( ).

§ 4º - Não é permitido utilizar as **2 (duas)** últimas senhas cadastradas;

§ 5º - É mandatório alterar a senha a cada **120 (cento e vinte)** dias;

§ 6º - Estabelecer um padrão de criação e utilização de **senhas fortes,** no intuito de evitar que pessoas mal-intencionadas as descubram e se passem por outras pessoas, acessando, por exemplo: contas de correio eletrônico, aplicações/sistemas e dispositivos de **TIC;** sites indevidos ou informações privilegiadas departamentais/institucionais, como se fosse o proprietário;

§ 7º - Evitar a utilização na criação das senhas de: nomes, sobrenomes, nomes de contas de **USUÁRIOs** e dados de membros da família, números de documentos, números de telefone, placa de carros e datas comemorativas; sequência do teclado (exemplo: asdfg123); palavras do dicionário, nomes de times de futebol, de música, de produtos, de personagens de filmes etc.;

§ 8º - Utilizar: números aleatórios; vários e diferentes tipos de caracteres; caracteres especiais; substituir uma letra por número com semelhança visual; a primeira, a segunda ou a última letra de cada palavra. Exemplo: com a frase "O Cravo brigou com a Rosa debaixo de uma sacada" você pode gerar a senha ***"?OCbcaRddus"*** (o sinal de interrogação foi colocado no início para acrescentar um símbolo à senha);

§ 9º - Senha temporária é uma senha gerada pelos **administradores de TIC** para um determinado **USUÁRIO** e que, só é válida até o primeiro acesso autenticado bem-sucedido. Podem ser entregues ao titular, ao **representante de USUÁRIOs** da localidade/departamento ou a outrem por procuração registrada em cartório;

§ 10 - Em caso de esquecimento da senha, uma senha temporária pode ser fornecida eletronicamente por esta **DTI** após o solicitante fornecer informações de caráter pessoal e não públicas que permitam sua autenticação;

§ 11 - É recomendado a adoção de ***“listas críticas”*** de senhas, de forma a evitar que os **USUÁRIOs** criem senhas fáceis de serem descobertas;

§ 12 - Cabe aos **administradores de TIC** adotar procedimentos de administração de senhas específicos para o seu ambiente computacional, observando estas normas;

§ 13 - As aplicações não devem armazenar a senha do **USUÁRIO,** mas sim utilizar o *hash* criptográfico da mesma, sendo recomendado o uso do algoritmo *SHA 256* ou superior.

Artigo 13 - No caso de interrupção de vínculo do **USUÁRIO** com a **Fundação CASA/SP,** a conta será inativada e todos os acessos serão removidos/bloqueados de imediato.

Artigo 14 - No caso de transferência de lotação do **USUÁRIO,** a conta será bloqueada de forma temporária, até a formalização do pedido do novo **representante de USUÁRIOs** para liberação dos acessos devidos.

CAPÍTULO V - CADASTRO E AUTORIZAÇÃO DE ACESSO

Artigo 15 - A **DTI** realiza os cadastros, alterações, bloqueios, concessões, revogações e fornece aos **USUÁRIOs** autorizados contas de acesso que permitem o uso de ativos de **TIC,** aplicações/sistemas de informação e recursos computacionais como, por exemplo, rede corporativa.

§ 1º - As referidas contas de acesso são fornecidas exclusivamente para que os **USUÁRIOs** possam executar suas atividades laborais;

§ 2º - Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um **incidente** de segurança da informação, cabendo uma análise da infração pela **DTI** e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP.**

Artigo 16 - A autorização e o nível permitido de acesso ativos/serviços de **TIC** da **Fundação CASA/SP** é feita com base em perfis que definem o nível de privilégio dos **USUÁRIOs.**

Artigo 17 - O acesso à ativos/serviços de **TIC** é fornecido a critério da **DTI,** que define permissões baseadas nas necessidades laborais dos **USUÁRIOs.**

Artigo 18 - Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores de cada **USUÁRIO.** Solicitações devem ser encaminhadas a **DTI** e/ou ao **gestor de sistema,** para uso de ativos e aplicações/sistemas desejados.

Artigo 19 - É responsabilidade do gestor imediato e/ou do **gestor de sistema** solicitar a **DTI** a concessão aos colaboradores que necessitem de novos acessos conforme mudanças em suas atividades laborais.

§ 1º - Solicitar a **DTI** e/ou ao **gestor de sistema** a remoção/revogação de acessos aos colaboradores quando necessário;

§ 2º - Solicitar a **DTI** concessão a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;

§ 3º - Solicitar a **DTI** e/ou ao **gestor de sistema** a remoção/revogação de acessos quando houver o encerramento do contrato com terceiros/prestadores de serviços contratados que operacionalizam ativos/sistemas de informação.

CAPÍTULO VI – DISPOSIÇÕES FINAIS

Artigo 20 - 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 21 - 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 22 - 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 23 - 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/ou virtual 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 24 - 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 25 - 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 26 - Os casos de **não conformidade** serão avaliados pela **DTI** e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP.**

Artigo 27 - Esta **OS** entra em vigor na data de sua publicação.

CAPÍTULO VII – 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