

ORDEM DE SERVIÇO DTI Nº 002/2023

Dispõe sobre a política de gestão de ativos 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, Capítulo VII - Seção I - Art. 46, Seção II Art. 50;
- 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. NIST SP 800-53 v4 - AC-3, AC-4, AC-16, AC-20, CM-8, CM-9, MP-2, MP-3, PL-4, PM-5, PS-6, RA-2, SC-16;
- VIII. ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos - A.8 (A.8.1., A.8.2., A.8.3.);
- IX. Framework de segurança cibernética do CIS 8; Salvaguarda 1,2 e 3;
- X. Framework Information Technology Infrastructure Library - ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI - Gestão da Segurança da Informação;
- XI. 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 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. **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. **ativos intangíveis:** a marca e a reputação da empresa/instituição, por exemplo; aquilo que não é constituído de um bem material físico;
- VII. **ativos físicos:** dispositivos/equipamentos que compõem os recursos de TIC, como desktops, dispositivos móveis, mídias removíveis, equipamentos de comunicação e conectividade, entre outros e suas respectivas instalações;
- VIII. **ativos de software:** os programas, sistemas, ferramentas e utilitários adquiridos ou desenvolvidos pela **Fundação CASA/SP** e que fazem parte das atividades laborais e de execução das medidas socioeducativas;
- IX. **ativos de serviço:** dispositivos/equipamentos de infraestrutura como eletricidade, ventilação, controle de umidade, entre outros;
- X. **ativos de informação:** são dados em tráfego ou armazenados em aplicações/sistemas de TIC, estejam estes em formato lógico (elétrico, magnético ou ótico) ou físico (impressos);
- XI. **disponibilidade:** os ativos devem estar disponíveis para o desempenho de suas funções nominais;
- XII. **confiabilidade:** a capacidade dos controles e monitoramentos de manter a confiança do desempenho esperado, reduzindo os riscos e aproveitando as oportunidades.;
- XIII. **custo:** gerenciamento do orçamento operacional capaz de contribuir para otimização do custo de produção e obtenção do retorno financeiro planejado;
- XIV. **acesso:** ato ou permissão para ingressar, transitar, conhecer, consultar, manipular e utilizar os ativos de informação;
- XV. **controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;
- XVI. **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;
- XVII. **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 - INTRODUÇÃO E PRINCÍPIOS GERAIS

Artigo 4º - A gestão de ativos de TIC dentro da **Fundação CASA/SP** é fundamental para que se alcance os objetivos e cumprimento das políticas de gestão de TIC. Diante disso, se faz necessário a gestão de software e hardware, afim de criar procedimentos capazes de garantir a disponibilidade e integridade dos ativos em uso, preservando assim a informação gerada ou mantida.

§ 1º - Esta OS deve estar alinhada com às políticas de gestão de TIC da DTI.

§ 2º - Esta OS deve estar alinhada com a gestão de continuidade de negócios em nível organizacional.

§ 3º - O processo de mapeamento de ativos de TIC estrutura e mantém um registro de ativos, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

§ 4º - As rotinas de inventário e mapeamento de ativos de TIC devem ser orientadas para a identificação na instituição, a fim de manter o escopo da organização mapeado e documentado.

§ 5º - O processo de mapeamento de ativos de TIC deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

§ 6º - Estabelecer padrões para que os ativos de TIC da Fundação CASA/SP sejam identificados; definir responsabilidades apropriadas para proteção e divulgação da gestão dos ativos de TIC da instituição, por meio do estabelecimento e manutenção de inventários, além de assegurar que o ciclo de vida dos ativos seja realizado e gerenciado para garantir a segurança da informação e o atendimento as legislações, normas e boas práticas recomendadas.

CAPÍTULO IV - DIRETRIZES E CONFORMIDADE

Artigo 5º - Do inventário.

§ 1º - Informações ou ativos de TIC de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado:

- I. Os ativos de TIC da Fundação CASA/SP devem ser inventariados, claramente identificados e registrados;
- II. A categorização do inventário deve ser aprovada pelas partes apropriadas ou autoridade de autorização;
- III. A Divisão de Patrimônio, Infraestrutura e Logística (DPIL) com o apoio da DTI; têm a responsabilidade de realizar periodicamente os inventários e armazenar os resultados por um período pré-estabelecido para fins de auditoria interna;
- IV. Periodicamente deve haver uma revisão pela DTI para assegurar que os ativos de TIC estejam em conformidade com o inventário;
- V. A instituição empregará o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo hardware ou software;
- VI. O inventário também deverá incluir atualizações ou remoções do sistema de informação.

Artigo 6º - Das responsabilidades dos administradores de TIC:

- I. Identificar potenciais ameaças aos ativos de TIC;
- II. Identificar vulnerabilidades dos ativos de TIC;
- III. Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de TIC ou de grupos de ativos em um relatório;
- IV. Avaliar os riscos dos ativos de TIC ou do grupo de ativos;
- V. Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na OS sobre Política de Gestão de Identidade e Controle de Acesso e catalogadas no sistema de gestão de ativos;
- VI. Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.

Artigo 7º - A criticidade dos ativos de TIC da instituição é determinado pelo:

- I. Requisitos legais;
- II. Pelo valor financeiro;
- III. Pelo seu potencial de agregar valor ao negócio e
- IV. Por sua vida útil.

Artigo 8º - Todos os **ativos de informação** devem ser classificados de acordo com sua criticidade. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos **ativos de informação** da **Fundação CASA/SP** devem ser classificados de acordo com a legislação pertinente, podendo ser classificado em uma das seguintes categorias:

- I. **Ultrassecreta:** São passíveis de classificação como ultrassegredos, dentre outros, dados, informações ou documentos referentes à soberania e à integridade territorial nacionais, a planos e operações, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade ou do Estado;
- II. **Secreta:** São passíveis de classificação como segredos, dentre outros, dados, informações ou documentos referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse institucional, a assuntos restritos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança da **Fundação CASA/SP**, da sociedade ou do Estado;
- III. **Reservada:** São passíveis de classificação como confidenciais, dentre outros, dados, informações ou documentos que, no interesse da **Fundação CASA/SP**, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da instituição, da sociedade ou do Estado.

Artigo 9º - Os ativos de TIC serão rotulados e manuseados com base nos procedimentos apropriados de classificação de informações usados pela organização.

Artigo 10 - Da manipulação de mídia:

- I. A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de **ativos de informação** usado pela instituição;
- II. A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos apropriados;
- III. A mídia contendo informações confidenciais e internas do **Fundação CASA/SP** devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

Artigo 11 - Do uso aceitável.

§ 1º - Padrões ou diretrizes para o **uso aceitável** de ativos devem ser documentados para indicar o que os **USUÁRIOS** dos ativos de TIC podem ou não fazer. Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis (vide **OS DTI nº 006/2023**):

- I. Uso do dispositivo/computador e dos sistemas de informação e comunicação;
- II. Uso de softwares e dados;
- III. Uso da Internet e e-mail;
- IV. Uso do telefone;
- V. Uso de equipamentos e materiais de escritório.

Artigo 12 - Como requisito de acesso ao ativo de TIC e como componente do treinamento de conscientização de segurança, todos os **USUÁRIOS**, sejam servidores ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis.

Artigo 13 - Os novos projetos de desenvolvimento ou para novas aquisições, devem seguir os padrões estabelecidos nesta OS.

§ 1º - Caso não seja possível a adequação, recurso técnico ou processo, a DTI deve documentar estar ciente, para fins de auditoria.

CAPÍTULO V - DISPOSIÇÕES FINAIS

Artigo 14 - 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 15 - 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 16 - 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 17 - 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 18 - 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 19 - 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 20 - Os casos de **não conformidade** serão avaliados pela DTI e, caso necessário, levados a autoridade máxima da **Fundação CASA/SP**.

Artigo 21 - Esta OS entra em vigor na data de sua publicação.

CAPÍTULO VI - 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