



**Governo do Estado de São Paulo**  
**Fundação Centro de Atendimento Socioeducativo ao Adolescente**  
**ATI - Assessoria de Tecnologia da Informação**

## INSTRUÇÃO

**Nº do Processo:** 161.00063320/2025-49

**Interessado:** FUNDACAO CASA, ATI - Assessoria de Tecnologia da Informação

**Assunto:** Política de Gestão de Serviços de TI

<b>Responsável</b>	Assessoria de Tecnologia da Informação - ATI
<b>Aprovado por:</b>	Gabinete da Presidência.
<b>Políticas Relacionadas</b>	Política de Governança de TI, Política de Segurança da Informação, Política de Uso Aceitável de TI, Política de Backup e Recuperação de Dados, Política de Serviços de Mensageria e Telefonia, Política de Gestão de Acessos
<b>Localização de armazenamento</b>	Processo SEI 161.00063320/2025-49
<b>Data da Aprovação</b>	Data da assinatura
<b>Data de revisão</b>	
<b>Versão</b>	1.0

### 1- PROPÓSITO

O objetivo desta política é garantir que os ativos de tecnologia da informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de TI estejam em vigor.

Para manter a segurança e continuidade do negócio da Fundação CASA-SP, em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização. Auxiliando também na recuperação de incidentes.

Os ativos de TI da Fundação CASA-SP devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um “dono”, no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

### 2- ESCOPO

- Esta política se aplica a todos os ativos de tecnologia da informação na Fundação CASA-SP.
- A classificação dos ativos de TI e o escopo desta política serão revisados periodicamente.

## 2- TERMOS E CONDIÇÕES

**Ativos de Tecnologia da Informação (TI)** – Conjunto de componentes tecnológicos que suportam os serviços e operações da organização, incluindo hardware (servidores, computadores, dispositivos móveis), software (sistemas operacionais, aplicativos), redes (roteadores, switches, cabeamento), bancos de dados e serviços de TI.

**Ativos físicos** – Recursos tangíveis de TI, como servidores, computadores e demais equipamentos essenciais para o processamento e armazenamento de informações.

**Bancos de dados** – Sistemas estruturados para armazenamento, gerenciamento e recuperação de informações de forma organizada.

**Dispositivos móveis** – Equipamentos portáteis, como smartphones e tablets, que permitem o acesso e gerenciamento de informações de forma remota.

**Endereço IP** – Identificador único atribuído a um dispositivo em uma rede baseada em protocolos IP, possibilitando sua localização e comunicação.

**Hardwares** – Componentes físicos que compõem os sistemas de TI, incluindo computadores, servidores, periféricos e outros dispositivos eletrônicos.

**Incidente** - Interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

**Mídia removível** – Dispositivos de armazenamento portáteis, como pen drives, discos externos e cartões de memória, que podem ser desconectados do ambiente de TI.

**Níveis de permissões** – Classificações de acesso que definem as autorizações dos usuários sobre os ativos de TI, de acordo com suas funções e responsabilidades.

**Proprietário do Ativo** – Responsável por definir a classificação, os riscos e as diretrizes de proteção dos ativos de TI, autorizando e supervisionando seu uso conforme os objetivos organizacionais.

**Script** – Conjunto de comandos automatizados utilizados para executar tarefas ou processos no ambiente de TI.

**Segmentação de Rede** – Prática de dividir a infraestrutura de rede em segmentos isolados para controlar o tráfego, restringir acessos e aumentar a segurança. A segmentação pode ser feita com VLANs, firewalls e listas de controle de acesso (ACLs), permitindo que determinados grupos de dispositivos ou usuários tenham comunicações restritas conforme regras definidas.

**Serviços** – Funcionalidades ou operações fornecidas pela TI que suportam as atividades e os processos da organização.

**Softwares** – Programas e aplicações que executam tarefas em sistemas de TI, facilitando a operação e a gestão dos ativos de TI.

**Versão de software** – Identificação (numérica ou codificada) que indica a edição ou atualização específica de um software.

### 3 - REFERÊNCIAS LEGAL E DE BOAS PRÁTICAS

Orientação	Seção
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
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
Norma 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.)

#### Declarações da política

Art. 1º. Fica instituída a Política de Gestão de Ativos de Tecnologia da Informação (TI) com a finalidade de estabelecer diretrizes, normas e responsabilidades para o gerenciamento do ciclo de vida dos ativos de tecnologia da informação, incluindo aquisição, registro, utilização, manutenção, monitoramento, descarte e segurança, garantindo a eficiência operacional, a conformidade com normas e regulamentos aplicáveis e a proteção dos recursos tecnológicos da Fundação CASA-SP.

Art. 2º. Esta Política de Segurança da Informação aplica-se a todas as unidades organizacionais da Fundação CASA-SP, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração.

### CAPÍTULO I DOS PRINCÍPIOS GERAIS

Art. 1º A Política de Gestão de Ativos de TI deve estar alinhada com a **Política de Segurança da Informação** e a **Política de Continuidade Operacional de TI** da Fundação CASA-SP.

Art. 2º As rotinas de inventário e mapeamento de ativos de TI devem ser orientadas para a identificação dos ativos de TI da Fundação CASA-SP, a fim de manter o escopo da organização mapeado e documentado.

Art. 3º O mapeamento e registro de ativos de TI subsidiará os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Art. 4º O processo de mapeamento de ativos de TI deve considerar, preliminarmente os objetivos estratégicos da Fundação CASA-SP, seus processos internos, os requisitos legais e sua estrutura organizacional.

Art. 5º Os seguintes ativos de TI devem ser considerados no processo de mapeamento de ativos de TI:

I. **Ativos físicos** – Equipamentos de infraestrutura, como servidores, projetores, storages, switches, roteadores, pontos de acesso, impressoras e dispositivos de backup, como fitas e storages externos;

II. **Bancos de dados** – Bases estruturadas e não estruturadas utilizadas para armazenamento e processamento de informações institucionais;

III. **Dispositivos móveis** – Equipamentos portáteis, como notebooks, tablets e smartphones corporativos;

IV. **Hardwares e periféricos** – Componentes internos de equipamentos de TI, como processadores, memórias e discos rígidos, e periféricos como mouses e teclados;

V. **Níveis de permissões e acessos** – Perfis de usuários, credenciais e regras de controle de acesso aos sistemas e ativos da Fundação CASA-SP;

VI. **Serviços de TI** – Serviços disponibilizados internamente ou por terceiros, como servidores de e-mail, sistemas de autenticação, VPNs, serviços em nuvem e aplicações SaaS (Software as a Service);

VII. **Softwares e licenças** – Aplicações utilizadas na Fundação CASA-SP, incluindo sistemas operacionais, ferramentas de produtividade e softwares licenciados;

VIII. **Sistemas internos** – Soluções desenvolvidas internamente para atender às necessidades específicas da Fundação CASA-SP, incluindo código-fonte, banco de dados e documentação associada;

IX. **Sistemas externos e serviços de terceiros** – Plataformas utilizadas pela Fundação CASA-SP, não hospedadas internamente;

X. **Ativos de Rede e Comunicação** – Equipamentos e configurações da rede corporativa, incluindo máquinas virtuais e IPs externos.

## **CAPÍTULO II DAS DIRETRIZES**

Art. 6º Os ativos de TI devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

Art. 7º A organização deverá utilizar da segmentação de rede para organizar seus ativos de TI.

Art. 10. A Assessoria de Tecnologia da Informação - ATI deve implementar o controle de acessos e privilégios mínimos para a administração dos ativos de TI.

Art. 11. A ATI deve adotar e fazer cumprir os níveis mínimos de disponibilidade de seus ativos de TI.

Art. 12. A Gerência de Suporte ao Usuário empregará o uso de mecanismos para identificar sistemas autorizados e não autorizados, incluindo hardware ou software.

Art. 13. A ATI deve assegurar que os ativos de TI inventariados possuam contrato de suporte em vigor, conforme criticidade e disponibilidade orçamentária.

Art. 14. A ATI empregará o uso de ferramentas de descoberta ativa ou passiva, conforme disponibilidade, para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

Art. 15. A Gerência de Suporte ao Usuário utilizará ferramentas de inventário de software, quando possível, em toda a Fundação CASA-SP para automatizar a descoberta e documentação do software instalado.

Art. 16. A ATI assegurará que exista um processo para lidar com ativos não autorizados.

Art. 17. A ATI utilizará de scripts e protocolos de segurança para o acesso e administração dos ativos de TI.

Art. 18. A Gerência de Infraestrutura e Segurança da Informação deverá elaborar e manter diagramas e demais documentações da arquitetura de rede da Fundação CASA-SP. A revisão destas documentações deverá ser realizada de forma periódica ou quando ocorrerem mudanças significativas, que possam impactar tais artefatos.

Art. 19. A Gerência de Infraestrutura e Segurança da Informação deverá garantir que a infraestrutura de rede da Fundação CASA-SP esteja atualizada. Deverá ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da Fundação CASA-SP.

Art. 20. O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação.

Art. 21. O inventário deve apresentar a quantidade de ativos em uso e disponíveis para alocação.

Art. 22. As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação pela Gerência de Suporte ao Usuário.

Art. 23. Para controle dos ativos de TI (por exemplo, desktops, laptops, servidores, tablets), quando aplicável, será utilizado o código de patrimônio.

Art. 24. O registro de ativos de TI resultante do processo de mapeamento deve conter, sempre que aplicável, os seguintes dados:

I. Código de Patrimônio;

II. Nome do ativo;

III. Descrição detalhada da sua finalidade e funcionalidade;

IV. Responsável pelo ativo (proprietário ou gestor);

V. Data de aquisição, implementação ou incorporação ao ambiente de TI;

VI. Versão ou configuração específica;

VII. Classificação quanto à criticidade e sensibilidade da informação associada;

VIII. Localização física ou lógica do ativo;

IX. Tempo de vida útil estimado e cronograma de substituição, quando aplicável;

X. Registros de manutenção, atualização ou mudanças significativas;

XI. Dependências e relacionamentos com outros ativos.

### **CAPÍTULO III - DAS RESPONSABILIDADES DO RESPONSÁVEL PELO ATIVO DE TI**

Art. 25. Identificar potenciais ameaças aos ativos de TI;

Art. 26. Identificar vulnerabilidades dos ativos de TI;

Art. 27. Consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de TI em um relatório;

Art. 28. Avaliar os riscos dos ativos de TI ou do grupo de ativos de TI.

Art. 29. Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na **Política de Gestão de Acessos**.

Art. 30. Os processos em torno do gerenciamento de mudança e de configuração estão descritos na **Política de Gestão de Mudanças**.

Art. 31. Todos os ativos de TI devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

## **CAPÍTULO IV - CRITICIDADE DO ATIVO DE INFORMAÇÃO**

Art. 32. A criticidade dos ativos de TI críticos da Fundação CASA-SP é determinada pelo:

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

## **CAPÍTULO V - MANIPULAÇÃO DE MÍDIA**

Art. 33. Mídias de armazenamento removíveis com dados da Fundação CASA-SP só podem ser transportadas externamente com autorização da ATI.

Art. 34. 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, após a devida formatação.

Art. 35. Para prosseguimento antes da eliminação deve ser realizada a remoção segura de todos os dados sensíveis armazenados nos ativos de armazenamento.

Art. 36. Métodos de exclusão de dados confiáveis, como formatação segura ou destruição física de mídias de armazenamento devem ser utilizados.

## **CAPÍTULO VI - USO ACEITÁVEL**

Art. 37. Padrões ou diretrizes para o uso aceitável de ativos para indicar o que os usuários dos ativos de TI podem ou não fazer estão descritas na **Política de Uso Aceitável de TI** e na **Política de Serviços de Mensageria e Telefonia**.

## **CAPÍTULO VIII - DISPOSIÇÕES GERAIS**

Art. 38. Toda aquisição, parceria ou proposta de doação de ativos de TI deve passar pela análise técnica da Assessoria de Tecnologia da Informação – ATI.

Art. 39. Esta política será revisada periodicamente, conforme a necessidade e evolução das melhores práticas de governança de TI, segurança da informação e mudanças na legislação aplicável.

Art. 40. Alterações na Política deverão ser submetidas à aprovação do Gabinete da Presidência.

São Paulo, na data da assinatura digital.

**Raelen Bego Luiz**  
Chefe de Gabinete

**Leandro Timossi de Almeida**  
Assessor da Presidência



Documento assinado eletronicamente por **Leandro Timossi de Almeida, Assessor da Presidência II**, em 13/03/2025, às 16:33, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



Documento assinado eletronicamente por **Raelen Bego Luiz, Chefe de Gabinete**, em 18/03/2025, às 22:30, conforme horário oficial de Brasília, com fundamento no [Decreto Estadual nº 67.641, de 10 de abril de 2023](#).



A autenticidade deste documento pode ser conferida no site [https://sei.sp.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0059099237** e o código CRC **00AB6062**.