



## NORMAS ORGANIZACIONAIS

Norma Organizacional Nº v.2/2025 - TERRACAP/COINT/COTIN/DIGTI

Brasília-DF, 28 de outubro de 2025.

**GOVERNO DO DISTRITO FEDERAL**  
**COMPANHIA IMOBILIÁRIA DE BRASÍLIA**  
Gabinete Assessoria dos Órgãos Colegiados  
**CONSELHO DE ADMINISTRAÇÃO DA TERRACAP**

Dispõe sobre a Política de Governança de Tecnologia e Inovação (PGTI) na Companhia Imobiliária de Brasília – TERRACAP.

**O CONSELHO DE ADMINISTRAÇÃO DA COMPANHIA IMOBILIÁRIA DE BRASÍLIA – TERRACAP**, no uso das atribuições que lhe confere o Estatuto Social, e considerando a necessidade de aprimorar continuamente suas práticas de governança, integridade, sustentabilidade e inovação, em alinhamento com as diretrizes da Lei nº 13.303/2016 (Lei das Estatais), da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), do Decreto nº 40.015/2019 (dispõe sobre a obrigatoriedade de elaboração e publicação dos Planos Diretores de Tecnologia da Informação e Comunicação), do Decreto nº 45.539/2024 (que regulamenta a Lei nº 13.303/2016 no âmbito do DF), bem como as diretrizes do Programa de Governança e da Política de Gestão de Riscos da Terracap, **RESOLVE:**

### **CAPÍTULO I**

#### **DA FINALIDADE**

**Art. 1º** Esta política visa estabelecer princípios, diretrizes, conceitos e responsabilidades para a governança da Tecnologia e Inovação da Companhia Imobiliária de Brasília – Terracap e suas subsidiárias, a fim de assegurar o alinhamento estratégico da TI com a estratégia e plano de negócios da empresa, a criação de valor público, a promoção da sustentabilidade e a conformidade com as melhores práticas de governança, risco e compliance.

### **CAPÍTULO II**

#### **DOS FUNDAMENTOS**

**Art. 2º** Esta política está fundamentada nos seguintes instrumentos normativos e padrões de referência:

- I. Lei nº 13.303, de 30 de junho de 2016 (Lei das Estatais);
- II. Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD);
- III. Decreto nº 40.015, de 14 de agosto de 2019 (Obrigatoriedade de elaboração e publicação dos Planos

Diretores de Tecnologia da Informação e Comunicação;

IV. Decreto nº 45.539, de 28 de abril de 2024 (Regulamenta a Lei nº 13.303/2016 no âmbito do DF);

V. Programa de Governança da Terracap;

VI. Política de Gestão de Riscos da Terracap;

VII. Padrões e normas reconhecidos internacionalmente, como ISO 37000 (Governança), ISO 27001 (Segurança da Informação), ISO 37301 (Compliance), COSO ERM, ITIL (Information Technology Infrastructure Library) e COBIT (Control Objectives for Information and Related Technology).

### **CAPÍTULO III**

#### **SIGLAS E DEFINIÇÕES**

**Art. 3º** São adotadas as seguintes siglas e definições:

I. **LGPD** - Lei Geral de Proteção de Dados Pessoais;

II. **PGTI** - Política de Governança de Tecnologia e Inovação;

III. **PETI** - Plano Estratégico de Tecnologia da Informação;

IV. **PDTI** - Plano Diretor de Tecnologia da Informação;

V. **TI** - Tecnologia da Informação - ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar e disseminar informações;

VI. **CTSI** - Comitê de Tecnologia e Segurança da Informação: comitê instituído no âmbito da Terracap com competência para acompanhar as ações estratégicas, organizacionais, operacionais e de segurança da informação definidas pelo PDTI, sejam executadas na forma estabelecida;

VII. **PCTI** - Plano de Continuidade de Tecnologia da Informação: conjunto de estratégias que visa assegurar a continuidade dos serviços de Tecnologia da Informação e Comunicação, abrangendo planos de recuperação, de contingência e gestão de crises em casos de desastres;

VIII. **PRD** - Plano de Recuperação de Desastres: documento que descreve como uma organização deve recuperar-se após um desastre;

IX. **OTR** - Objetivo de Tempo de Recuperação: tempo máximo que um sistema, aplicação, rede ou computador pode ficar inativo após um incidente de falha ou desastre;

X. **POR** - Objetivo do Ponto de Recuperação: quantidade máxima de dados que uma organização pode perder após um desastre;

XI. **Unidade de Tecnologia da Informação**: Unidade de nível hierárquico mais elevado na organização, com competência atribuída por Regimento Interno, responsável pela gestão especializada da tecnologia da informação;

XII. **Alta administração**: Diretoria Colegiada (DIRET) e CONAD (Conselho de Administração);

XIII. **ESG**: é uma sigla em inglês e significa Environmental, Social and Governance (Ambiental, Social e Governança). Esse termo abrange um conjunto de práticas voltadas para a preservação do meio ambiente, responsabilidade com a sociedade e governança empresarial;

XIV. **Governança de TI**: Conjunto de princípios, diretrizes, normas, processos, estruturas organizacionais e instrumentos de controle que visam avaliar, direcionar e monitorar o uso da TI a fim de assegurar que as decisões e as ações relacionadas à gestão e ao uso de TI estejam integradas às necessidades institucionais, contribuindo para o cumprimento da missão e o alcance das metas organizacionais, a criação de valor público e o alinhamento com os princípios ESG;

XV. **Gestão de TI**: responsável pelo planejamento, desenvolvimento, execução e monitoramento das atividades de TI em consonância com a direção definida pela função de governança de TI a fim de atingir os objetivos corporativos;

XVI. **ITIL** (Information Technology Infrastructure Library): Conjunto de práticas detalhadas para o gerenciamento de serviços de TIC que se concentram no alinhamento dos serviços de TI com as necessidades dos negócios;

XVII. **COBIT** (Control Objectives for Information and Related Technology): O COBIT é um arcabouço de regras amplamente reconhecido como um padrão global para a governança de TI e é utilizado por empresas em todo o mundo para melhorar a gestão de seus recursos de TI;

XVIII. **ISO/IEC 38500**: É uma norma internacional que estabelece os princípios para a governança corporativa de TI;

XIX. **Inteligência Artificial Generativa (IAG)**: É um ramo da inteligência artificial projetado para criar conteúdos como textos, áudios, imagens, vídeos e códigos de software que se baseia em modelos computacionais avançados, que aprendem padrões a partir de grandes volumes de dados;

XX. **Inteligência Artificial Generativa Pública (IAG - pública)**: É a IAG não indicada pela Terracap para uso;

XXI. **Inteligência Artificial Generativa Corporativa (IAG - corporativa)**: É a IAG autorizada pela Terracap para uso corporativo;

XXII. **Aprendizado de Máquina**: é uma aplicação de IA que tem como objetivo ensinar uma máquina a realizar uma tarefa específica e fornecer resultados precisos identificando padrões.

## **CAPÍTULO IV DOS PRINCÍPIOS**

**Art. 4º** A governança da Tecnologia e Inovação na Terracap será pautada pelos seguintes princípios, em consonância com o Programa de Governança da Companhia e as melhores práticas de mercado:

I. **Alinhamento Estratégico**: As iniciativas e operações de TI devem estar alinhadas aos objetivos estratégicos, planos de negócio e necessidades da empresa, contribuindo diretamente para a consecução da missão institucional e dos princípios ESG;

II. **Criação de Valor** : A TI deve estar orientada para geração valor para a Companhia e para os cidadãos do Distrito Federal e para a sociedade, considerando os impactos econômicos, sociais e ambientais;

III. **Gestão por Resultados**: As ações relacionadas à governança de TI deverão ser implantadas considerando mecanismos para a medição e o monitoramento das metas de TI, sempre que possível, permitindo que a função de governança possa validar e direcionar as ações de TI, com foco na eficiência, eficácia e efetividade;

IV. **Conformidade (Compliance)**: As atividades de TI devem estar em conformidade com a legislação vigente, regulamentações aplicáveis, e requisitos contratuais e políticas internas da Terracap;

V. **Transparência**: As decisões e ações relacionadas à governança de TI devem ser transparentes, claras e comunicadas às partes interessadas relevantes, promovendo o acesso à informação e a prestação de contas;

VI. **Integridade**: A governança de TI deve promover e sustentar a ética e a probidade em todas as suas ações, prevenindo fraudes, corrupção e conflitos de interesse, em alinhamento com o Programa de Integridade da Terracap e a ISO 37000;

VII. **Confiabilidade**: A TI deve garantir a segurança, disponibilidade e integridade das informações e sistemas, minimizando incertezas e assegurando a continuidade dos serviços essenciais;

VIII. **Melhores Práticas de TI**: As atividades da TI serão pautadas pelo conjunto de diretrizes, práticas e ferramentas reconhecidas como padrões globais como COBIT, ISO/IEC 38500, ITIL, ISO 27001 (Segurança da Informação) e COSO ERM (Gestão de Riscos Corporativos);

IX. **Melhoria Contínua**: Buscar o aperfeiçoamento contínuo dos processos, serviços e recursos de TI, visando aumentar a eficiência, eficácia, segurança e inovação;

X. **Inovação**: A TI deve impulsionar soluções para a otimização de processos de negócio, por meio da

proposição e implementação de novas soluções de tecnologia voltadas a resultados;

**XI. Accountability (Prestação de Contas):** Os responsáveis pela governança de TI devem prestar contas de sua atuação de forma clara, concisa e tempestiva;

**XII. Responsabilidade Corporativa:** A governança de TI deve zelar pela viabilidade econômico-financeira da empresa, com ética e transparência, e pela perenidade da Terracap, considerando os impactos de suas decisões no ambiente e na sociedade;

**XIII. Sustentabilidade:** As decisões e projetos de TI devem considerar os impactos ambientais e sociais, buscando soluções que promovam a eficiência energética, a redução de resíduos eletrônicos e o desenvolvimento de tecnologias que apoiem os objetivos de sustentabilidade da Terracap.

## **CAPÍTULO V DOS PAPÉIS E RESPONSABILIDADES**

### **Art.5º Compete ao Conselho de Administração (CONAD) da Terracap:**

- I. Aprovar esta PGTI e suas revisões;
- II. Definir as diretrizes de governança para a área de TI, em alinhamento com o Planejamento Estratégico Corporativo e os princípios ESG.
- III. Supervisionar a implementação das ações decorrentes da presente PGTI

### **Art. 6º Compete à Diretoria Colegiada da Terracap (DIRET):**

- I. Implementar a PGTI;
- II. Monitorar a efetividade e o desempenho da PGTI;
- III. Aprovar o Plano Diretor de Tecnologia da Informação (PDTI).

### **Art. 7º Compete ao Comitê de Tecnologia e Segurança da Informação (CSTI):**

- I. Propor a priorização de projetos e submeter o PDTI para aprovação pela Diretoria Colegiada;
- II. Acompanhar e monitorar a implementação do PDTI;
- III. Propor ações para auxiliar no efetivo cumprimento da PGTI e do PDTI;

### **Art. 8º Compete à Controladoria Interna (COINT):**

- I. Coordenar ações de governança, integridade e inovação em tecnologia da informação, de modo a promover a sua integração no âmbito da Terracap e subsidiárias;
- II. Articular, propor, promover e acompanhar a implementação de mecanismos e boas práticas de governança, integridade e inovação em tecnologia da informação na Terracap, em consonância com as diretrizes estabelecidas pelo Conselho de Administração;
- III. Avaliar a conformidade dos processos e controles de TI com a PGTI e demais normativos aplicáveis.

### **Art. 9º Compete à Coordenação de Tecnologia da Informação e Inovação (COTIN):**

- I. Coordenar e executar as políticas, processos e serviços de TI, em conformidade com a PGTI;
- II. Adotar medidas de segurança da informação e proteção dos dados da empresa, em alinhamento com a Política de Segurança da Informação (POSIC) e o Programa de Governança em Privacidade (PGP);
- III. Elaborar e submeter à aprovação do Comitê de Tecnologia e Segurança da Informação (CSTI) o PDTI e suas revisões;

### **Art. 10 Compete ao Comitê de Gestão de Riscos (COGER):**

- I. Difundir as práticas de Gestão de Riscos;
- II. Zelar pelo cumprimento da Política de Gestão de Riscos;

III. Promover a disseminação da cultura da gestão de riscos no âmbito da Terracap;

**Art. 11 Compete à Auditoria Interna (AUDIT):**

I. Avaliar, de forma independente, a eficácia dos controles internos e dos processos de governança de TI, incluindo a conformidade com a PGTI, a Política de Segurança da Informação (POSIC) e a Política de Gestão de Riscos;

II. Realizar auditorias nos sistemas e ambiente de TI, com ênfase na segurança da informação, integridade dos dados e continuidade dos negócios;

III. Reportar os resultados das auditorias de TI ao CONAD e COAUD, propondo recomendações para aprimoramento

**Art. 12 Compete aos Usuários:**

I. Utilizar os recursos de TI de forma ética, responsável e segura, seguindo as políticas, normas e procedimentos estabelecidos, incluindo as diretrizes de uso de IAG;

II. Reportar incidentes de segurança da informação e não conformidades relacionadas à TI.

## CAPÍTULO VI

### DAS DIRETRIZES PARA O PLANO DIRETOR DE TI (PDTI)

**Art. 13** Os instrumentos de planejamento de TI (PETI/PDTI) serão elaborados em consonância com o Planejamento Estratégico Corporativo aprovado, o Plano de Negócios e princípios ESG da Terracap.

**Art. 14** O planejamento da TI deve contar com ampla participação das partes interessadas, enunciando objetivos para o período de vigência.

**Art. 15** As ações de TI devem ser conduzidas mediante a utilização de instrumentos adequados de avaliação, direção e monitoramento, conforme prescrevem as boas práticas em Governança de TI (COBIT, ITIL, ISO/IEC 38500).

**Art. 16** Os objetivos de TI, sempre que possível, devem ser monitorados por indicadores, desdobrados em projetos, executados segundo processos, sendo orientadores de toda a atuação da TI.

**Art. 17** O PDTI abrangerá as contratações identificadas e o orçamento necessário para o período de vigência.

## CAPÍTULO VII

### DAS DIRETRIZES PARA O USO DE INTELIGÊNCIA ARTIFICIAL GENERATIVA(IAG) E APRENDIZADO DE MÁQUINA NA COMPANHIA

**Art. 18** O uso de Inteligência Artificial Generativa (IAG) e Aprendizado de Máquina na Terracap deve ser guiado por princípios éticos, de segurança, privacidade e responsabilidade, visando maximizar os benefícios e mitigar os riscos.

**Art. 19** Ferramentas de IAG-Corporativa podem ser usadas para automatizar atividades de análise de informações e geração de conteúdo, desde que sempre com revisão e validação humana.

**Art. 20** As decisões assistidas por modelos de IAG devem ser avaliadas pelo usuário para garantir a assertividade, imparcialidade, objetividade e absterem-se de viés ou preconceito.

**Art. 21** A IAG-corporativa deve ser utilizada considerando aspectos de segurança da informação, privacidade de dados corporativos e de terceiros, e em conformidade com a LGPD e a Política de Segurança da Informação (POSIC).

**Art. 22** Todos os colaboradores, ao usar serviços de IAG corporativa, devem pautar sua conduta pelas

orientações contidas na norma GOV03 – Código de Conduta e Integridade.

**Art. 23** Os dados utilizados para treinamento de modelos internos de aprendizado de máquina devem ser cuidadosamente selecionados, anonimizados ou pseudonimizados para proteger a privacidade dos indivíduos, e devem ser auditáveis para garantir a rastreabilidade.

**Art. 24** Devem ser implementadas práticas de segurança robustas para garantir que os dados de treinamento não sejam acessados ou alterados por partes não autorizadas.

**Art. 25** O treinamento de modelos deve ser conduzido de forma ética, evitando a introdução de vieses que possam resultar em discriminação, preconceito ou decisões injustas.

**Art. 26** Os usuários devem ser informados quando estão interagindo com sistema de IA, garantindo a transparência e a compreensão da natureza da interação.

## CAPÍTULO VIII

### DAS DIRETRIZES PARA GESTÃO DE RISCOS DE TI

**Art. 27** A Terracap fomentará a cultura de gestão de riscos de TI como fator essencial para implantar estratégias e planos de TI, em alinhamento com a Política de Gestão de Riscos da Companhia.

**Art. 28** A unidade de TI deve adotar uma abordagem estruturada para identificar, analisar, avaliar, tratar e monitorar os riscos setoriais de TI, abrangendo as atividades de rotina e considerando o potencial impacto ao bom andamento das atividades e aos objetivos estratégicos.

**Parágrafo único.** Os riscos de TI incluem, mas não se limitam a: riscos de cibersegurança (ataques, vazamentos de dados), riscos de continuidade de negócios (falhas de sistemas, desastres), riscos de conformidade (LGPD, regulamentações), riscos de obsolescência tecnológica, riscos de desempenho e riscos associados ao uso de novas tecnologias, como o viés algorítmico em sistemas de IA.

## CAPÍTULO IX

### DAS DIRETRIZES PARA GESTÃO DE SERVIÇOS DE TI

**Art. 29** Os serviços de TI devem ser relacionados e formalizados em um catálogo de serviços, com definição clara de responsabilidades e níveis de serviço.

**Art. 30** Os níveis de serviço devem ser revisados periodicamente para garantir a adequação às necessidades do negócio e às expectativas dos usuários.

**Art. 31** Os processos operacionais, a infraestrutura e as aplicações devem ser gerenciados de forma a cumprir os níveis de serviço estabelecidos, garantindo a eficiência e a qualidade.

**Art. 32** Os serviços oferecidos aos usuários, sempre que necessário, serão acompanhados de uma Política de Uso que abrangerá: a forma mais indicada para utilização do serviço, as restrições de utilização do serviço, o nível de segurança e responsabilidades do usuário.

**Art. 33** As Políticas de Uso serão divulgadas por meio de e-mail institucional e outros canais de comunicação interna.

**Art. 34** Com vistas a manter a continuidade da prestação de serviços de TI em caso de desastres e sinistros na infraestrutura física e lógica de TI, a COTIN deve formular, implantar e testar regularmente o Plano de Continuidade de TI (PCTI).

## CAPÍTULO X

### DAS DIRETRIZES PARA O PROVIMENTO DE SOLUÇÕES DE TI

**Art. 35** Para os fins do disposto nesta Política, o provimento de soluções de TI compreende as seguintes modalidades:

I. **Desenvolvimento:** construção de soluções, com recursos próprios ou de terceiros, para atender as necessidades específicas da Terracap;

II. **Aquisição:** adoção de soluções construídas externamente por meio de contratação, recebimento de outros órgãos do DF e entidades ou utilização de software livre.

**Art. 36** Deverá ser adotada a solução que melhor atender a Companhia considerando os custos e benefícios, o alinhamento estratégico e os impactos ESG.

**Art. 37** A concepção de soluções deve estar pautada na otimização de processos de trabalho, na integração de soluções e na reutilização de dados e componentes, promovendo a eficiência e a inovação.

**Art. 38** Na aquisição ou desenvolvimento de soluções de TI devem ser levados em consideração os critérios de segurança da informação, desempenho, usabilidade, privacidade de dados e sustentabilidade (e.g., eficiência energética, ciclo de vida do produto).

**Art. 39** Previamente à implantação devem ser realizados os testes necessários para assegurar o correto funcionamento e a aderência das soluções às regras de negócio e aos requisitos especificados.

**Art. 40** Deve-se identificar as lacunas de conhecimento dos usuários previamente à implantação de novas soluções de TI, sugerindo, quando necessário, capacitação e treinamento.

## CAPÍTULO XI

### DAS DIRETRIZES PARA GESTÃO DE AQUISIÇÕES DE TI

**Art. 41** As aquisições de TI devem estar alinhadas às estratégias, planos e prioridades institucionais, considerando a alocação orçamentária necessária à realização das iniciativas planejadas e em conformidade com Regulamento Interno de Licitações e Contratações da Companhia Imobiliária de Brasília- TERRACAP e demais normas pertinentes.

**Art. 42** A escolha da solução deve considerar o custo-benefício, a compatibilidade com o ambiente tecnológico da instituição e os requisitos de segurança da informação e sustentabilidade.

**Art. 43** As contratações devem prever, sempre que possível, indicadores de desempenho, níveis de serviço (SLA) e formas de monitoramento contínuo da execução contratual.

**Art. 44** As contratações de TI devem envolver, obrigatoriamente:

I. Área de TI (responsável técnica);

II. Área requisitante (demanda);

III. Área administrativa (execução contratual).

**Art. 45** Ficam dispensadas da obrigatoriedade de elaboração do Estudo Técnico Preliminar (ETP) e de previsão no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) as seguintes situações, desde que observados os princípios de planejamento, economicidade e transparência previstos no RILC:

I. Contratações emergenciais, em que se caracterize situação de urgência capaz de ocasionar prejuízos ou comprometer a continuidade de serviços essenciais, nos termos da legislação vigente;

II. Aquisições ou contratações com valor global inferior ao previsto para compra por dispensa de licitação constante no RILC, desde que não recorrentes, de baixo impacto e justificadas tecnicamente quanto à sua necessidade e compatibilidade com o ambiente tecnológico institucional;

III. Contratações decorrentes de exigências legais, judiciais ou normativas, cujo atendimento seja obrigatório e urgente, devidamente evidenciado por documentação oficial.

**Parágrafo único.** Essas exceções não eximem a instituição da observância aos princípios da legalidade, eficiência, economicidade, impessoalidade, publicidade e transparência, devendo todos os atos ser

formalmente registrados e arquivados.

**Art. 46** Contratações de bens e serviços de tecnologia da informação de uso específico e restrito a um grupo restrito de usuários, como softwares especializados ou ferramentas de nicho, deverão ser conduzidas diretamente pela respectiva unidade demandante com participação da área de TI na análise técnica e validação da solução proposta

## **CAPÍTULO XII**

### **DAS DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO**

**Art. 47** A informação é um dos principais ativos da organização e deve ser utilizada e protegida de forma adequada contra riscos, ameaças, acessos não autorizados e danos. Para isso, é fundamental que todas as unidades e colaboradores compreendam e assumam sua responsabilidade na proteção das informações, assegurando a confidencialidade, integridade e disponibilidade da informação de acordo com as normas, condutas e procedimentos adotados na empresa, em conformidade com a Política de Segurança da Informação (POSIC) e a ISO 27001.

**Art. 48** Deve-se estabelecer uma estratégia de segurança da informação alinhada aos objetivos e estratégias do negócio, contemplando as necessidades atuais e futuras da organização, e abordando os riscos cibernéticos de forma proativa.

**Art. 49** Todas as ações de segurança da informação que demandem recursos financeiros devem ser devidamente previstas no PDTI, garantindo o planejamento e a destinação adequada dos investimentos necessários à proteção das informações.

## **CAPÍTULO XIII**

### **DOS INDICADORES E MÉTRICAS DE GOVERNANÇA DE TI**

**Art. 50** A efetividade da Política de Governança de Tecnologia e Inovação será monitorada e avaliada por meio de indicadores e métricas, que deverão ser periodicamente revisados e reportados às instâncias de governança.

**Parágrafo único.** Os indicadores e métricas poderão abranger, mas não se limitar aos temas de estratégia, riscos, conformidade e Integridade, desempenho dos serviços e otimização de recursos.

## **CAPÍTULO XIV**

### **DAS DISPOSIÇÕES FINAIS**

**Art. 51** Os casos omissos ou excepcionais relativos a esta Política serão analisados pela Diretoria Colegiada (DIRET).

**Art. 52** Esta Política entra em vigor na data de sua publicação.

Karina Nunes Alves Costa  
Chefe da DIGTI

De acordo,  
Júlio Cezar Schettini Henriques



Documento assinado eletronicamente por **JÚLIO CEZAR SCHETTINI HENRIQUES - Matr.0002401-5, Coordenador(a) de Tecnologia da Informação e Inovação**, em 04/11/2025, às 14:20, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



A autenticidade do documento pode ser conferida no site:  
[http://sei.df.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&verificador=185634034)  
verificador= **185634034** código CRC= **0AAF3E7A**.

"Brasília - Patrimônio Cultural da Humanidade"  
ST SAM BLOCO F - CEP 70620-000 - DF  
613342943