	SANTOS PORT AUTHORITY		
	Instrumento Normativo de Processo		**Código: TIC-110**
	Diretoria Responsável: **Presidência**	Unidade Responsável: **Superintendência de Tecnologia da Informação**	Elaboração: **Supervisão de Governança de TI**
	Início da vigência: **03/05/2023**	Aprovação: **Decisão DIREXE nº 169.2023**	Validação: **Superintendência de Tecnologia da Informação**
PROCESSO: Gerir Processo de Software			Versão: **3.0.6**

INSTRUMENTO NORMATIVO - GERIR PROCESSO DE SOFTWARE

SUMÁRIO

1. OBJETIVO DO PROCESSO 4

2. ABRANGÊNCIA 4

3. FUNDAMENTAÇÃO 4

4. DEFINIÇÕES 4

5. ARCABOUÇO LEGAL 7

6. DISPOSIÇÕES NORMATIVAS 7

6.1. DIRETRIZES GERAIS 7

6.1.1. Regramentos e restrições 7

6.1.2. Ciclo de Vida 8

6.1.3. Fatores Críticos de Sucesso 9

6.1.4. Aquisições de soluções de TIC 10

6.2. MACRO FASE DEMANDA 11

6.2.1. Disposições Gerais 11

6.3. MACRO FASE PLANEJAMENTO 12

6.4. MACRO FASE EXECUÇÃO 18

6.5. MACRO FASE SUSTENTAÇÃO E EVOLUÇÃO 22

6.6. MACRO FASE MONITORAMENTO E CONTROLE 23

7. PONTOS DE CONTROLE 24

8. PAPÉIS E RESPONSABILIDADES 25

8.1. GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS (GEDES) 25

8.2. GERÊNCIA DE INFRAESTRUTURA DE DADOS (GERID) 25

8.3. SUPERVISÃO DE OPERAÇÃO E SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO (SEOTI): 26

8.4. SUPERVISÃO DE GOVERNANÇA DE TI (SEGTI) 27

8.5. PATROCINADOR 27

8.6. REPRESENTANTE DA ÁREA DE NEGÓCIO 28

8.7. LÍDER TÉCNICO DE PROJETO 28

8.8. EQUIPE DE PROJETO 29

8.9. DONO DO PROCESSO DE NEGÓCIO (CLIENTE) 29

8.10. USUÁRIO CHAVE 30

8.11. USUÁRIO FINAL 31

8.12. ENCARREGADO DE DADOS PESSOAIS 31

9. DISPOSIÇÕES FINAIS 32

10. ANEXOS 32

1. OBJETIVO DO PROCESSO

O processo de software tem como principal objetivo fomentar a melhoria na qualidade, controle e segurança da informação durante o ciclo de vida de sistemas de informação, por meio de indicação de boas práticas que servem como referência na execução de atividades ligadas ao planejamento, desenvolvimento, implantação e sustentação desses sistemas.

2. ABRANGÊNCIA

Este Instrumento Normativo aplica-se a toda demanda de software que necessite passar por um processo de planejamento, desenvolvimento/parametrização e implantação.

As práticas aqui determinadas devem ser seguidas por todos os empregados, colaboradores, fornecedores e clientes que utilizam software da Companhia para desempenhar suas funções.

3. FUNDAMENTAÇÃO

Este documento está fundamentado na Política de Gestão de Serviços de TIC da SPA, na Política de Segurança e Privacidade, e no SGPI, no Regulamento Interno de Licitações e Contratos – RILC em vigor e nas boas práticas abaixo:

Referência	Descrição
ISO/IEC 27001:2013	*Information technology -- Security techniques -Information security Management systems --Requirements*
ISO/IEC 27701:2019	*Information technology --Security techniques - Privacy Information Management System (PIMS)*
CIS v8 – item 16	*Application Software Security*

4. DEFINIÇÕES

TERMO	DESCRIÇÃO
Ambiente de desenvolvimento	Ambiente que os desenvolvedores utilizam para construir o software.
Ambiente de Produção	Ambiente onde os usuários finais acessam o software para utilização.
Ambiente de testes e homologação	Ambiente onde parte dos testes serão executados, com o intuito de certificar que as funcionalidades requisitadas foram desenvolvidas/configuradas corretamente.
Análise Estática	Análise realizada sem executar um programa. Tem por objetivo encontrar vulnerabilidades e demais problemas na aplicação, e normalmente é executada durante a fase de revisão de código dentro do ciclo de vida de desenvolvimento de sistemas.
Análise dinâmica	É um procedimento de teste que faz parte do processo de depuração de software e usado para avaliar um programa durante a execução em tempo real. É aplicado durante a fase de desenvolvimento

Anonimização	É uma técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados anonimizados, que não podem ser associados a nenhum indivíduo específico.
Descarte de dados	O descarte de dados é a eliminação de dados de uma organização conforme as definições do negócio, ou em decorrência de término de prazo de retenção dos dados.
Desenvolvimento de Software	Atividade de construção ou parametrização de um software para manutenção ou atualização dele.
Desenvolvimento de Software Seguro	Atividade de construção ou parametrização de um software para manutenção ou atualização dele, utilizando técnicas que minimizem a existência de vulnerabilidades que possam ser exploradas.
Documento de Oficialização de Demanda - DOD	Documento que contém o detalhamento da necessidade da Unidade de Gestão Requisitante da Solução.
Escopo do produto	Descrição detalhada do objetivo do produto.
ETIR	Equipe de Tratamento e Resposta a Incidentes.
Fuzzing	É uma técnica para testar o software usando entradas inválidas ou inesperadas para um programa ou função em um programa, logo verificando os resultados para ver se o programa falha ou age de forma inapropriada.
GO/No-GO	É um marco que formalmente aprova o início da sua efetiva entrada de um sistema em produção.
Parametrização	É a ação de estabelecer parâmetros de processamento de um determinado sistema a fim de atender necessidades específicas.
Partes interessadas	Envolvidos que de alguma forma afetam ou são afetados, positiva ou negativamente, pela demanda.
PDTI	Plano Diretor de Tecnologia da Informação: Instrumento de diagnóstico, planejamento e gestão dos recursos e processos de TI que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade por um determinado período.
Plataforma de aplicação	Conjunto de ativos que podem ser usados para alavancar o reuso e o rápido desenvolvimento de novas aplicações. No nosso caso, a plataforma define o ambiente operacional, a arquitetura e a forma de apresentação (desktop, ou web, por exemplo) de como a aplicação será oferecida ao requisitante.
Privacidade por desenho/ Privacidade por padrão	Privacidade por Design e por Default ou Privacy by Design and Default é um conceito que defende que todo projeto de elaboração de um produto ou serviço, seja no mundo físico ou virtual, tenha como base respeito à privacidade das informações utilizadas, com ampla segurança de dados.
Pseudoanonimização	o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.
Relatório de Impacto à Proteção de Dados Pessoais	Documentação do controlador [SPA] que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
Release	É a entrega de um ou mais Incrementos do Produto prontos, gerados pela Equipe de Desenvolvimento, para que sejam utilizados.

Requisitos básicos	Requisitos básicos necessários para o atendimento da demanda, normalmente relacionados a questões de negócio, de recursos humanos, de desempenho, legais, sociais, ambientais e culturais.
Requisitos de infraestrutura	Requisitos de infraestrutura para a implantação da solução de software.
Requisitos de sustentação	Requisitos para a execução do monitoramento e do suporte do sistema.
Requisitos funcionais	Requisitos relacionados as funcionalidades e serviços do sistema para o atendimento da demanda.
Requisitos não-funcionais	Requisitos relacionados às propriedades e restrições do sistema, como segurança, desempenho, espaço em disco etc.
Retenção de Dados	A retenção de dados é o armazenamento contínuo de dados de uma organização conforme as definições do negócio.
SGPI	Sistema de Gestão de Segurança da Informação e Privacidade
SI&P	Sigla para representar Segurança da Informação e Privacidade
Teste de Penetração	É um método que avalia a segurança de um sistema de computador ou de uma rede, simulando um ataque de uma fonte maliciosa.
Varredura de vulnerabilidade	É o processo que visa identificar e relatar problemas de segurança (conhecidos como vulnerabilidades) que afetam sistemas.

5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
Resolução nº 41 CGPAR	2022	Dispõe sobre o planejamento e implementação de práticas de governança de Tecnologia da Informação (TI) que atendam de forma adequada os padrões usualmente reconhecidos nesta área, pelas empresas estatais federais.
Lei nº 13.709	2018	Lei Geral de Proteção de Dados.

6. DISPOSIÇÕES NORMATIVAS

6.1. DIRETRIZES GERAIS

6.1.1. Regramentos e restrições

Todo e qualquer processo de construção ou de parametrização de Software deve ser precedido de planejamento e estar alinhado com o PDTI vigente da Companhia.

Para tal, devem ser observados os normativos de:

a) Gestão de Demandas (onde é feita a verificação de alinhamento ao PDTI);
b) Plano Diretor de TI (PDTI), e;
c) Regulamento Interno de Licitações e Contratos - RILC, em destaque seção sobre contratações de TIC.

O desenvolvimento e integração de soluções de software corporativas deve ser restrito à Gerência de Desenvolvimento de Sistemas (GEDES) e terceiros por ela contratados para tal.

O uso de linguagens de programação que auxiliam ferramentas como Power BI, PowerAutomate/PowerApps, Excel ou scripts em Python, R, dentre outros, é permitido pelos empregados da SPA, desde que:

a) não contrarie os normativos da SPA ou a legislação vigente;

b) não implique no desenvolvimento de uma solução de software, por exemplo: com telas, bases de dados, integrações e/ou acessos por diversos usuários internos ou externos

c) haja consentimento da Superintendência de Tecnologia da Informação (SUPTI) via solicitação de autorização por chamado por parte do empregado, devidamente justificada.

Os softwares desenvolvidos devem respeitar a regulamentação referente à propriedade intelectual, licenças etc.

Os softwares desenvolvidos por empregados ou prestadores de serviços para a Companhia devem ser de propriedade exclusiva dela. É proibido copiar, divulgar e utilizar estes softwares sem prévia autorização escrita da Companhia.

O desenvolvimento de software deve estar segregado logicamente em distintos ambientes, incluindo bases de dados, de maneira que se evite incidentes com o acesso e manuseio indevido de dados.

Para cada processo de software, devem ser criados ao menos os seguintes ambientes:

a) desenvolvimento;

b) homologação, e;

c) produção.

É dever da GEDES definir perfis de acesso e quem poderá acessar os diversos ambientes de sistemas e códigos-fonte. Tais definições devem:

a) ser de conhecimento dos desenvolvedores, e;

b) seguir as diretrizes do normativo de gestão de acesso de sistemas vigente.

6.1.2. Ciclo de Vida

O ciclo de vida de um software consiste das seguintes macro-fases:

a) Demanda (Escopo e Viabilidade);

b) Planejamento (Plano de Projeto);

c) Execução;

d) Implantação e estabilização; e

e) Sustentação e evolução.

A transição de fases até a chegada à Sustentação e evolução depende de:

a) parecer técnico da GEDES, e;

b) aprovação do(s) dono(s) de processo(s) de negócio afetados (doravante, cliente(s)).

A GEDES deve instituir padrões e/ou metodologias para:

a) desenvolvimento de sistemas da informação, inclusive considerando critérios de desenvolvimento seguro;

b) testes
c) monitoramento do projeto
d) carga de dados
e) manuais e treinamentos
f) arquitetura de software
g) requisitos de continuidade
h) sustentação da aplicação
i) versionamento de código-fonte de sistemas;

j) mensuração do tamanho de software, e;

k) nomenclaturas e documentação de:

i) arquivos;

ii) código-fonte, e;

iii) manuais de procedimentos.

Estes padrões devem ser seguidos em todo processo de software.

É ideal que as funções de análise de sistemas e codificação sejam segregadas, de modo a evitar a concentração do conhecimento da lógica em uma única pessoa. Caso isso não seja possível deve ser realizada passagem de conhecimento para os envolvidos no processo de desenvolvimento, além da documentação.

6.1.3. Fatores Críticos de Sucesso

São considerados fatores críticos de sucesso para a execução do processo de software:

a) o patrocínio da Diretoria Executiva e da Superintendência de TI;

b) o comprometimento dos envolvidos no processo;

c) o entendimento e alinhamento de expectativas entre os envolvidos;

d) a ampla divulgação do processo pela empresa;

e) a utilização de boas práticas de mercado;

f) a capacitação técnica do pessoal envolvido na execução do processo;

g) a manutenção de uma infraestrutura e recursos modernos e adequados às necessidades de negócio;

h) o escopo ser definido com clareza;

i) a análise e avaliação de riscos de Segurança da Informação & Privacidade e os controles de redução de risco;

j) Em caso de a solução envolver Dados Pessoais, a elaboração do Relatório de Impacto à Proteção de Dados Pessoais;

k) o acesso às informações necessárias para o desenvolvimento das aplicações estar claro para os envolvidos;

l) o prazo ser compatível com o escopo;

m) o treinamento prévio dos usuários e a prevenção da substituição deles ao longo do projeto;

n) a disponibilidade dos usuários para executarem as atividades de implementação;

o) a não ocorrência de interrupções na execução do projeto, respeitando o planejamento;

p) a promoção de reuniões periódicas de acompanhamento;

q) a agilidade na aprovação da documentação do projeto, considerando o prazo apresentado no cronograma, para não afetar o andamento das demais atividades.;

r) A especificação de procedimentos para implantação da solução (gestão de mudanças);

s) A Análise de Impacto no Negócio para determinação dos parâmetros de continuidade da solução e seu impacto no negócio.

6.1.4. Aquisições de soluções de TIC

O processo de software pode ser viabilizado por meio de aquisições de soluções de TI. Neste cenário, devem ser observados:

a) a obrigação dos fornecedores em seguir os padrões e metodologias instituídos a partir deste processo de software;

b) o Regulamento Interno de Licitações e Contratos da Companhia (RILC);

c) a comunicação e concordância com os requisitos que serão objetos de monitoramento e análise crítica visando à garantia de atendimento às expectativas;

d) A existência de Acordo de Licença, propriedade do código e direitos de propriedade intelectual apropriados;

e) Requisitos contratuais para um projeto seguro, práticas de código seguro e testes;

f) Fornecimento de um modelo de ameaça aprovado para o desenvolvedor externo;

g) Teste de aceitação relativos à qualidade e exatidão dos itens entregues;

h) Fornecimento de evidência de que os princípios de segurança foram utilizados para proteger contra presença de conteúdo malicioso e contra a presença de vulnerabilidades conhecidas;

i) Acordos de garantia para o caso do código fonte não estiver mais disponível;

j) Direitos autorais para auditar os controles e processos de desenvolvimento.

Ferramentas consideradas aplicativos de escritório, e Software como Serviço que não necessitem cargas de dados de informações históricas podem ser adquiridas pela Gerência de Infraestrutura de Dados (GERID).

Serviços de TIC em nuvem que são específicos do negócio e sem necessidade de desenvolvimento, integrações, infraestrutura, manutenção, configuração e administração tecnológica, devem, preferencialmente, ser geridos por outras unidades organizacionais. Para isso:

a) Seu planejamento de aquisição deve ser acompanhado pela área de tecnologia da informação;

b) Todo o planejamento de aquisição/contratação deve seguir o padrão corporativo para aquisição de itens de TIC.

O apoio técnico na execução de atividades do processo de software poderá ser objeto de contratação, desde que os trabalhos sejam supervisionados exclusivamente por empregados da própria Companhia.

Não é permitido que uma empresa contratada para realizar a métrica de um software seja também contratada para o seu desenvolvimento.

6.2. MACRO FASE DEMANDA

6.2.1. Disposições Gerais

FASE – RECEPÇÃO DA DEMANDA	
ATIVIDADES	**REGRAS/DIRETRIZES**
REQUISIÇÃO DE SOFTWARE	A recepção da demanda é o momento em que a Unidade de Gestão requisitante oficializa sua necessidade de software. A identificação deve ser: a) oficializada pela Unidade de Gestão requisitante, por meio de um Documento de Oficialização de Demanda (DOD), seguindo as práticas vigentes no normativo de gestão de demandas de TI; e, b) encaminhada à GEDES para que seja iniciado o processo de software.

6.3. MACRO FASE PLANEJAMENTO

A fase de planejamento caracteriza-se pelo conjunto de atividades que descrevem a especificação e dimensionamento da demanda, alocação de responsáveis, elaboração da visão do produto de software, especificação dos requisitos de desenvolvimento, infraestrutura e segurança e registro do backlog do produto.

FASE – LEVANTAMENTO DE REQUISITOS	
Esta fase deve conter o entendimento da demanda de software de modo a possibilitar a decisão sobre a solução mais adequada e viável para atender as necessidades de negócio.	
ATIVIDADES	**REGRAS/DIRETRIZES**
DEFINIÇÃO DE REQUISITOS BÁSICOS	**1)** Os requisitos de software devem ser definidos de forma viável e otimizada, visando atender às necessidades da Companhia com riscos e custos minimizados. **2)** Recomenda-se que sejam executadas as seguintes atividades para definição dos requisitos de software: a) a definição da visão de software (escopo e requisitos); b) a análise do processo de negócio, e; c) estabelecimento dos parâmetros de desempenho e atendimento; d) a estimativa inicial do tamanho de software, quando se tratar de desenvolvimento por terceiros. **3)** A estimativa inicial do tamanho de software deve ser realizada por meio da Análise de Pontos de Função, seguindo o padrão formalizado pela Companhia ou as boas práticas mais atuais de SISP e IFPUG. **4)** Definir os controles de Segurança da Informação & Privacidade (Análise e avaliação de Riscos de SI&P). **5)** Em caso de Dados Pessoais, definir os controles e/ou ações necessárias para redução de riscos à privacidade.

FASE – LEVANTAMENTO DE REQUISITOS	
Esta fase deve conter o entendimento da demanda de software de modo a possibilitar a decisão sobre a solução mais adequada e viável para atender as necessidades de negócio.	
ATIVIDADES	**REGRAS/DIRETRIZES**
	6) Definir requisitos de continuidade de negócio (Análise de Impacto ao Negócio), conforme apresentado na norma vigente que versa sobre Continuidade de Negócio.
DEFINIR OS CONTROLES DE SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE	**7)** Quando da definição de requisitos do produto, considerar os seguintes requisitos de segurança da Informação e privacidade: a) Utilização de autenticação de múltiplos fatores para usuários que estejam em ambiente externo; b) Utilização de componentes de terceiros, que façam parte do inventário de componentes (ou que tenham condições de fazer parte); c) Utilização de mecanismos de criptografia para transferência de informações (inclusive transferência de arquivos em lote) para terceiros (complementarmente à autenticação). **8)** Deverão ser considerados durante a fase de planejamento conceitos de desenvolvimento seguro: corrigir falhas de segurança durante o fluxo natural de desenvolvimento, em vez de realizar verificações de segurança apenas no final do processo. Envolve a especificação e aplicação de requisitos de segurança de informação e proteção à privacidade desde a definição de requisitos até a sustentação como: a) Definição de linha de base de segurança; b) Treinamento; c) Utilização de componentes de terceiros que sejam confiáveis.

FASE – LEVANTAMENTO DE REQUISITOS	
Esta fase deve conter o entendimento da demanda de software de modo a possibilitar a decisão sobre a solução mais adequada e viável para atender as necessidades de negócio.	
ATIVIDADES	**REGRAS/DIRETRIZES**
	d) Utilização de módulos ou serviços controlados para componentes de segurança da aplicação (gestão de identidade, criptografia, auditoria de logs). e) Manutenção de inventário de componentes de terceiros, incluindo o rastreamento em busca de vulnerabilidades e necessidades de atualização. f) Modelagem de ameaças (SI&P) para definir um plano de resposta a incidentes e/ou inclusão no plano de resposta a incidentes. g) Testes de segurança i) Análise estática ii) Análise dinâmica iii) Varredura de vulnerabilidade iv) Fuzzing v) Teste de penetração vi) Descarte e retenção de dados **9)** Quando o desenvolvimento da aplicação envolver tratamento de dados pessoais, deverão ser observadas obrigatoriamente as seguintes diretrizes vigentes que tratam de dados pessoais com foco em: a) **<u>Privacidade por desenho;</u>**

FASE – LEVANTAMENTO DE REQUISITOS	
Esta fase deve conter o entendimento da demanda de software de modo a possibilitar a decisão sobre a solução mais adequada e viável para atender as necessidades de negócio.	
ATIVIDADES	**REGRAS/DIRETRIZES**
	b) **<u>Privacidade por padrão;</u>** c) **<u>Anonimização e pseudoanonimização;</u>** d) **<u>Compartilhamento, transferência e divulgação de Dados Pessoais.</u>** **10)** Deverá ser adotado procedimento de mascaramento de dados para todo dado classificado como confidencial, de acordo com as diretrizes de Segurança e Privacidade e SGPI em normas vigentes, limitando a exposição deste tipo de dados para usuários sem privilégios. Logs de acesso e transações, devem ser confidenciais, seguindo o a norma vigente de Classificação da Informação. **11)** As diretrizes dispostas no documento vigente que trata de Controle de Acesso, devem ser consideradas de modo que as funcionalidades desenvolvidas em um software sejam acessadas apenas por pessoal com autorização para tal, de forma a prevenir mudanças não planejadas
UTILIZAÇÃO DE COMPONENTES DE TERCEIROS	**12)** Dentre o levantamento de outros requisitos, deve ser avaliada a necessidade de utilização de componente / bibliotecas de terceiros. Quanto a este ponto, deve observar: A Gestão de Componentes de Terceiros (inclusive bibliotecas e estruturas) é composto por um inventário de componentes (ou lista de materiais) não pertencentes ou não elaborados pela SPA. Uma vez estabelecido o inventário, é aconselhado fazer a gestão, dentro das possibilidades, a fim de mantê-lo atualizado não somente em relação aos seus itens, mas também

FASE – LEVANTAMENTO DE REQUISITOS	
Esta fase deve conter o entendimento da demanda de software de modo a possibilitar a decisão sobre a solução mais adequada e viável para atender as necessidades de negócio.	
ATIVIDADES	**REGRAS/DIRETRIZES**
	em relação aos riscos de cada um de seus itens e as atualizações. Resumidamente, visa gerenciar e catalogar componentes de terceiros para: a) Identificar riscos nos componentes b) Mantê-los atualizados e confiáveis O inventário deve ser revisado periodicamente para que os riscos destes componentes sejam controlados.
DEFINIÇÃO DE VIABILIDADE	**13)** A Análise de Viabilidade de Software deve: a) basear-se nos requisitos do software; b) seguir o modelo de Estudo Técnico Preliminar (ETP) do RILC; c) contemplar o estudo das soluções alternativas afim de averiguar sua viabilidade (técnica e econômica); e, d) definir a que melhor atende satisfatoriamente os requisitos definidos.

FASE – PLANEJAMENTO DA ESTRATÉGIA DE EXECUÇÃO (PLANO DE PROJETO)	
ATIVIDADES	**REGRAS/DIRETRIZES**
DEFINIÇÃO DA ESTRATÉGIA DE EXECUÇÃO	**14)** Para definir a Estratégia de Execução, deve-se: a) escolher a estratégia de execução do projeto;

	b) definir os controles de Segurança da Informação & Privacidade (Análise e avaliação de Riscos de SI&P); c) Em caso de Dados Pessoais, definir os controles e/ou ações necessárias para redução de riscos à privacidade; d) verificar a infraestrutura disponível para o funcionamento do software e planejar atualizações;

6.4. MACRO FASE EXECUÇÃO

FASE – REALIZAÇÃO DA ESTRATÉGIA DE EXECUÇÃO	
Para a fase de Realização da Estratégia de Execução devem ser considerados os requisitos de negócio, funcionais e técnicos planejados nas fases anteriores.	
ATIVIDADES	**REGRAS/DIRETRIZES**
DESENVOLVIMENTO DE SOFTWARE	**1)** As seguintes atividades têm sua execução recomendada durante o desenvolvimento de software, considerando inclusive aspectos de SI&P: a) preparação dos ambientes; b) execução do desenvolvimento, quando couber; c) execução dos testes e documentação dos resultados; d) gerenciamento de aquisições, caso existam; e) documentação do desenvolvimento realizado; f) planejamento da implantação; g) planejamento de treinamentos e elaboração de manuais; h) homologação do sistema; i) medição do tamanho final do software; j) planejamento da implantação, sob os critérios de gestão de mudança; k) treinamentos.

FASE – REALIZAÇÃO DA ESTRATÉGIA DE EXECUÇÃO	
Para a fase de Realização da Estratégia de Execução devem ser considerados os requisitos de negócio, funcionais e técnicos planejados nas fases anteriores.	
ATIVIDADES	**REGRAS/DIRETRIZES**
TESTE DE APLICAÇÃO	**2)** O ambiente de homologação deve se aproximar, no que for possível (considerando as condições para tratamento de dados, em especial os pessoais), das características do ambiente de produção, considerando: a) processos de negócio e procedimentos; b) número de usuários; e, c) a estimativa de volume de transações. **3)** Quando da preparação do ambiente de testes, deverão ser executadas as seguintes rotinas: a) Aplicar nos dados de teste os mesmos procedimentos de controle de acesso aplicados em sistemas de aplicações operacionais; b) A cada teste deve ser obtida autorização para utilizar uma cópia da informação operacional; c) Após finalizar os testes, deve ser apagada a informação operacional; d) Registrar, para fins de trilha de auditoria, que uma cópia da informação operacional foi utilizada para testes. **4)** Novos sistemas e aplicações e seus respectivos upgrades e versões sucessoras devem ser testados tendo como critério os requisitos de segurança previamente definidos. Falhas encontradas devem ser corrigidas e a homologação está condicionada ao atendimento de todos os requisitos, inclusive os de segurança da informação e privacidade.

FASE – REALIZAÇÃO DA ESTRATÉGIA DE EXECUÇÃO	
Para a fase de Realização da Estratégia de Execução devem ser considerados os requisitos de negócio, funcionais e técnicos planejados nas fases anteriores.	
ATIVIDADES	**REGRAS/DIRETRIZES**
	5) Os testes de auditoria em sistemas de informação devem ser planejados e acordados entre as partes envolvidas de forma a minimizar o impacto sobre os processos de negócio.
DOCUMENTAÇÃO DO SOFTWARE	**6)** Todos os componentes da solução desenvolvida devem possuir a documentação mínima necessária para que seja possível: a) o posterior entendimento do software, e; b) a redução de retrabalhos, inconsistências e redundâncias. **7)** A documentação gerada para o sistema finalizado deve: a) seguir os padrões e boas práticas instituídos pela GEDES; b) ter suas versões controladas, e: c) ter informações suficientes para permitir: i) sua instalação; ii) sua operação; iii) seu uso, e; iv) sua manutenção.

FASE – IMPLANTAÇÃO E ESTABILIZAÇÃO	
Esta fase deve efetivar a implantação do software (desenvolvido ou adquirido) em seu ambiente de produção, para o seu uso efetivo, estabilizando a solução de acordo com o esperado para sua operação e o retorno dos usuários.	
ATIVIDADES	**REGRAS/DIRETRIZES**
IMPLANTAÇÃO / ESTABILIZAÇÃO DE SOFTWARE	**8)** As seguintes atividades têm sua execução recomendada durante a implantação e estabilização de software: a) planejamento do tratamento de incidentes inclusive os SI&P; b) preparação do ambiente de produção, sob os critérios de gestão de mudança; c) execução da implantação; d) monitoramento da implantação; e) gerenciamento das aquisições, e; f) realização das cargas de dados, quando couber.

6.5. MACRO FASE SUSTENTAÇÃO E EVOLUÇÃO

FASE – SUSTENTAÇÃO E EVOLUÇÃO	
Esta fase deve caracterizar a finalização do projeto e entrada da aplicação de melhoria contínua.	
ATIVIDADES	**REGRAS/DIRETRIZES**
SUSTENTAÇÃO E EVOLUÇÃO	**1)** Nesta fase, são obrigatórias as seguintes atividades: a) encerramento do projeto; b) manutenção e evolução do software, contemplando: i) suporte continuado aos usuários, conforme normativo de Gestão de Serviços de TIC; ii) atendimento de novos requisitos que surgem do próprio uso e de mudanças de processos no negócio.

6.6. MACRO FASE MONITORAMENTO E CONTROLE

FASE – MONITORAMENTO E CONTROLE	
O monitoramento e controle nos projetos de software busca garantir a verificação do que deve ser realizado no projeto, ou seja, acompanhar os processos que são executados com as suas atividades, identificando ações corretivas e preventivas, estabelecendo assim maneiras de tomada de decisão na gestão de projetos de software.	
ATIVIDADES	**REGRAS/DIRETRIZES**
MONITORAMENTO E CONTROLE	**1)** As fases anteriores à Sustentação e Evolução devem ser monitoradas e controladas, de forma que seja possível obter um entendimento do progresso do projeto e executar ações apropriadas para: a) manter a qualidade; b) rever o escopo e/ou; c) gerenciar os riscos, inclusive os de SI&P. **2)** A comunicação entre as partes interessadas do processo de software pode ser realizada por meio de reuniões e ferramentas de comunicação usuais como e-mail e mensageiros eletrônicos.

7. PONTOS DE CONTROLE

Indicador	Desvio de Escopo de Entregas
Descrição	Quantidade de entregas de um projeto
Periodicidade	Mensal
Polaridade	Quanto maior, melhor
Fonte	Reuniões de planejamento do desenvolvimento e de entrega
Cálculo	$X = Média\left(\frac{Qtde\ de\ funcionalidades\ entregues\ pelo\ projeto}{Qtde\ de\ funcionalidades\ planejadas\ pelo\ projeto}\right)\ x\ 100\%$
Observações	São consideradas como entregas as funcionalidades solicitadas dentro de uma release, projeto ou ainda as entregas solicitadas via Ordem de Serviço (OS).

Indicador	Desvio de Prazo para Entregas
Descrição	Apurar o desvio entre prazo de entregas (planejado vs realizado) para desenvolvimentos entregues.
Periodicidade	Mensal
Polaridade	Quanto menor, melhor
Fonte	Artefatos de planejamento / monitoramento de projetos da GEDES
Cálculo	$X = \left(\frac{Tempo\ real\ para\ uma\ release}{Tempo\ planejado\ de\ uma\ release}\right)$
Observações	Indicador deve ser feito por release / entrega. A linha de base do tempo planejado estará sujeita a atualizações em casos de alteração de escopo.

Indicador	Taxa de bugs de um sistema
Descrição	Quantidade de problemas de uma aplicação após a ida para produção
Periodicidade	Mensal
Polaridade	Quanto menor, melhor
Fonte	Sistema de Controle de Chamados
Cálculo	Soma da quantidade de bugs após publicação de aplicação
Observações	A forma de apuração é genérica por aplicativo, mas é aconselhado que tal indicador seja acompanhado juntamente com a versão de releases ou funcionalidades/entregas.

8. PAPÉIS E RESPONSABILIDADES

8.1. GERÊNCIA DE DESENVOLVIMENTO DE SISTEMAS (GEDES)

<table>
<tr><th colspan="2">Responsável por</th></tr>
<tr><td colspan="2">• Responsável pelo desenvolvimento e gestão de todo o ciclo de vida dos sistemas utilizados na Companhia.
• Analisar e direcionar os chamados;
• Para os casos de incidentes de natureza grave, comunicar os gerentes de TI, para a adoção de medidas em caráter emergencial;
• Para eventos ou incidentes de SI&P comunicar imediatamente a ETIR.</td></tr>
<tr><th colspan="2">RECEPÇÃO DA DEMANDA</th></tr>
<tr><th>Principais atividades</th><th>Responsável por</th></tr>
<tr><td>REQUISIÇÃO DE SOFTWARE</td><td>• Recepcionar nova demanda de software e iniciar o processo de desenvolvimento de Software;
• Definir líder técnico do projeto.</td></tr>
<tr><th colspan="2">SUSTENTAÇÃO E EVOLUÇÃO</th></tr>
<tr><th>Principais atividades</th><th>Responsável por</th></tr>
<tr><td>SUSTENTAÇÃO E EVOLUÇÃO</td><td>• Analisar e direcionar os chamados.</td></tr>
</table>

8.2. GERÊNCIA DE INFRAESTRUTURA DE DADOS (GERID)

<table>
<tr><th>Responsável por</th></tr>
<tr><td>• Assegurar o gerenciamento dos recursos de infraestrutura e segurança da informação;
• Preparar, liberar e manter os ambientes de sistemas;
• Apoiar:
  ○ a implantação de software; e,
  ○ atualizações e upgrades necessários de infraestrutura para a operação do software;
  ○ as atividades que requerem informações de infraestrutura e segurança da informação.
• Para eventos ou incidentes de SI&P comunicar imediatamente a ETIR.</td></tr>
<tr><th>PLANEJAMENTO</th></tr>
</table>

Principais atividades	Responsável por
LEVANTAMENTO DE REQUISITOS – DEFINIÇÂO DE VIABILIDADE	• Validar o estudo de viabilidade quanto à necessidade de infraestrutura física para implementação do projeto e em caso necessidade de aquisição de infraestrutura, dar parecer técnico para tal.
EXECUÇÃO	
Principais atividades	**Responsável por**
DESENVOLVIMENTO DE SOFTWARE	• Apoiar a equipe do Projeto na preparação dos ambientes de software.

8.3. SUPERVISÃO DE OPERAÇÃO E SOLUÇÕES DE TECNOLOGIA DA INFORMAÇÃO (SEOTI):

Responsável por	
• Responsável pela prestação de serviços de TIC aos clientes internos da Companhia, executando atividades durante todo o ciclo de vida dos ativos de TIC; • Apoiar nas atividades do ciclo de vida de desenvolvimento que requerem suporte na operacionalização; • Atualizar o catálogo de serviços, e • Coordenar o tratamento de incidentes; • Para eventos ou incidentes de SI&P comunicar imediatamente a ETIR.	
PLANEJAMENTO	
Principais atividades	**Responsável por**
LEVANTAMENTO DE REQUISITOS	• Entendimento dos requisitos iniciais para planejamento dos níveis mínimos de serviço a serem atendidos para a aplicação em questão; • Planejar o tratamento de incidentes.
EXECUÇÃO	
Principais atividades	**Responsável por**
IMPLANTAÇÃO / ESTABILIZAÇÃO DE SOFTWARE	• Após a entrada em produção da aplicação, devem ser incluídos os novos serviços no catálogo de serviços da SPA, bem como a definição, em conjunto com o dono do processo e a GEDES de definição e assinatura dos níveis mínimos de serviço a serem atendidos para o suporte da aplicação.

8.4. SUPERVISÃO DE GOVERNANÇA DE TI (SEGTI)

Responsável por	
• Responsável por fornecer o devido apoio ao planejamento do desenvolvimento/aquisição da solução de TI, avaliando a demanda encaminhada pela Unidade de Gestão requisitante no que tange o alinhamento do DOD ao PDTI.	
RECEPÇÃO DA DEMANDA	
Principais atividades	**Responsável por**
REQUISIÇÃO DE SOFTWARE	• Recepção e avaliação da requisição de software enviada pela área requisitante; • Encaminhar demanda de software para a GEDES.

8.5. PATROCINADOR

Responsável por	
• Garantir o sucesso do projeto e o apoio e comprometimento dos envolvidos; • aprovar os recursos necessários para a melhorar a produtividade; • vetar as decisões do Líder do Projeto e do Usuários Chave; • atestar o andamento do projeto; • tomar decisões em casos de desentendimentos e discordâncias.	
MONITORAMENTO E CONTROLE	
Principais atividades	**Responsável por**
MONITORAMENTO E CONTROLE	• Acompanhar o projeto de desenvolvimento da aplicação

8.6. REPRESENTANTE DA ÁREA DE NEGÓCIO

Responsável por
Equivalente ao papel Product Owner (PO) no modelo ágil, é o profissional responsável pelo gerenciamento do projeto por parte do cliente, devendo: • elaborar definições, metas e prazos, em acordo com o Líder Técnico do projeto; • realizar as interfaces com as partes interessadas, mantendo-as informadas sobre o andamento do processo de software; • analisar a viabilidade de implantação do software; • realizar o planejamento do processo de software, em acordo com o Líder Técnico; • coordenar as atividades de implantação; • ter autonomia para decisões do projeto de caráter estratégico; • fornecer informações para a elaboração de uma análise de risco à privacidade, caso o projeto envolva Dados Pessoais; • fornecer informações para a elaboração da Análise de Impacto ao Negócio.

PLANEJAMENTO	
Principais atividades	**Responsável por**
LEVANTAMENTO DE REQUISITOS	• Definir os requisitos de negócio a serem atendidos pela aplicação.

EXECUÇÃO	
Principais atividades	**Responsável por**
TESTES DE APLICAÇÃO	• Acompanhar / executar testes e homologação da aplicação.

8.7. LÍDER TÉCNICO DE PROJETO

Responsável por
Equivalente ao papel Scrum Master no modelo ágil, é responsável por coordenar a execução do processo de software, devendo: • elaborar definições, metas e prazos, em acordo com o Representante da Área de Negócio do projeto; • coordenar as atividades de desenvolvimento em conjunto com o Representante da Área de Negócio; • monitorar a execução do projeto; • planejar a implantação em conjunto com o Representante da Área de Negócio do projeto, considerando os aspectos em “Gestão de Mudanças” e coletando as aprovações necessárias quando necessário.
PLANEJAMENTO

Principais atividades	Responsável por
TODA A FASE	• Liderar a fase de planejamento, através do levantamento/revisão de requisitos e do desenvolvimento da Análise de Viabilidade de software
EXECUÇÃO	
Principais atividades	**Responsável por**
TODA A FASE	• Liderar a fase de execução através do desenvolvimento ou acompanhamento técnico (em caso de contratação de desenvolvimento), inclusive durante a fase de testes de aplicações. • Desenvolver ou ainda revisar a documentação, juntamente com a área de negócio; • Acompanhar / realizar o treinamento de usuários-chave; • Acompanhar a implantação da aplicação no ambiente de produção.
SUSTENTAÇÃO E EVOLUÇÃO	
Principais atividades	**Responsável por**
SUSTENTAÇÃO E EVOLUÇÃO	• Assumir a sustentação e evolução da aplicação após a entrada do software em produção.
MONITORAMENTO E CONTROLE	
Principais atividades	**Responsável por**
MONITORAMENTO E CONTROLE	• Controlar a execução das tarefas dentro do período previsto, nos níveis de qualidade e riscos previstos.

8.8. EQUIPE DE PROJETO

Responsável por
• Equipe formada por todas as pessoas que participam do projeto, sendo responsável por auxiliar os líderes do projeto no desenvolvimento de suas atividades.

8.9. DONO DO PROCESSO DE NEGÓCIO (CLIENTE)

Responsável por
Gestor da Unidade de Gestão Requisitante. É responsável por: • definir as necessidades de negócio;

• aprovar e validar os trabalhos realizados em cada fase;

PLANEJAMENTO	
Principais atividades	**Responsável por**
LEVANTAMENTO DE REQUISITOS	• Definir as necessidades de negócio
EXECUÇÃO	
Principais atividades	**Responsável por**
DESENVOLVIMENTO DE SOFTWARE	• tomar decisão final sobre indefinições, prioridades, alternativas e assuntos críticos referentes à funcionalidades, tratamento de erros, manutenção e evolução.

8.10. USUÁRIO CHAVE

Responsável por
O Usuário Chave participa efetivamente na definição dos processos, mapa de funcionalidades e capacitação para uso do sistema. Deve: • ter conhecimentos satisfatórios sobre todos os processos de seu departamento; • homologar a entrada do sistema em produção (Reunião GO/No-GO); • elaborar manual de usuários; e • ser responsável pela replicação dos treinamentos realizados.

EXECUÇÃO	
Principais atividades	**Responsável por**
TESTES DE APLICAÇÃO	• Apoiar na execução de testes da aplicação
DOCUMENTAÇÃO DO SOFTWARE	• Elaborar manuais de usuários

8.11. USUÁRIO FINAL

Responsável por
O usuário final é um operador do sistema e deve: • participar dos testes e treinamentos; • utilizar o software de acordo com suas funções; • reportar falhas encontradas; • sugerir melhorias.

EXECUÇÃO	
Principais atividades	**Responsável por**
TESTES DE APLICAÇÃO	• Apoiar na execução de testes da aplicação

SUSTENTAÇÂO E EVOLUÇÃO	
Principais atividades	**Responsável por**
SUSTENTAÇÃO E EVOLUÇÃO	• Reportar falhas encontradas • Propor melhorias

8.12. ENCARREGADO DE DADOS PESSOAIS

Responsável por
• Orientar e sugerir medidas de preservação da confiabilidade das informações tratadas bem como a preservação da privacidade no que se refere à dados pessoais. • Acompanhar nas fases levantamento de requisitos como orientador dos requisitos aplicáveis aos projetos, de forma que esses requisitos sejam observados, em tempo de planejamento.

PLANEJAMENTO	
Principais atividades	**Responsável por**
LEVANTAMENTO DE REQUISITOS	• Avaliar o Relatório de Impacto à Proteção de Dados, quanto ao tratamento de dados pessoais, riscos à privacidade e correspondente medidas de mitigação.

	• Propor medidas adicionais caso as indicadas na análise de risco à privacidade sejam insuficientes. • Aprovar o tratamento na forma indicada na análise de risco à privacidade, se de acordo.

9. DISPOSIÇÕES FINAIS

As exceções à este Instrumento Normativo devem ser:

a) encaminhadas para a Gerência de Desenvolvimento de Sistemas, e;

b) reportadas formalmente à Superintendência de Tecnologia da Informação para posterior definição do tratamento adequado.

10. ANEXOS

Não Aplicável.