

	<b>SANTOS PORT AUTHORITY</b>			
	<b>Instrumento Normativo de Processo</b>			<b>Código: TIC-140-014</b>
	Diretoria Responsável: <b>Presidência</b>	Unidade Responsável: <b>Gerência de Desenvolvimento de Sistemas</b>		Elaboração: <b>Supervisão de Governança de TI</b>
	Início da vigência: <b>05/08/2021</b>	Próxima revisão: <b>05/08/2023</b>	Aprovação: Decisão Direxe nº <b>318.2021</b>	Validação: <b>Superintendente de Tecnologia da Informação</b>
Processo: <b>Sistema de Gestão da Privacidade da Informação: Aquisição, Desenvolvimento e Manutenção de Software.</b>			Versão: <b>1.1</b>	

# Instrumento Normativo de Processo

## Sistema de Gestão da Privacidade da Informação Aquisição, Desenvolvimento e Manutenção de Softwares

## SUMÁRIO

<b>1. OBJETIVO .....</b>	<b>3</b>
<b>2. ABRANGÊNCIA.....</b>	<b>3</b>
<b>3. FUNDAMENTAÇÃO .....</b>	<b>3</b>
<b>4. DEFINIÇÕES .....</b>	<b>3</b>
<b>5. ARCABOUÇO LEGAL .....</b>	<b>4</b>
<b>6. DIRETRIZES .....</b>	<b>5</b>
<b>6.1. Diretrizes .....</b>	<b>5</b>
<b>6.2. Consenso / Aprovação .....</b>	<b>9</b>
<b>7. PAPÉIS E RESPONSABILIDADES.....</b>	<b>9</b>
<b>7.1. Da Unidade Responsável.....</b>	<b>9</b>
<b>7.2. Das Unidades Executoras .....</b>	<b>10</b>
<b>8. DISPOSIÇÕES FINAIS .....</b>	<b>10</b>
<b>9. ANEXOS.....</b>	<b>10</b>

## 1. OBJETIVO

Estabelecer as diretrizes para 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

Todos os sistemas corporativos que são utilizados em ambientes de produção na Santos Port Authority – SPA, e se aplica a todos os empregados, os cedidos, os estagiários e os terceirizados que executem atividades nas instalações da Companhia.

## 3. FUNDAMENTAÇÃO

Este documento está fundamentado na Política de Segurança e Privacidade, e SGPI da SPA, em vigor.

## 4. DEFINIÇÕES

Termo	Descrição
<b>Ambiente de desenvolvimento</b>	Ambiente que os desenvolvedores utilizam para construir o <i>software</i> .
<b>Ambiente de Produção</b>	Ambiente onde os usuários finais acessam o <i>software</i> para utilização.
<b>Ambiente de testes e homologação</b>	Ambiente onde parte dos testes serão executados, com o intuito de certificar que as funcionalidades requisitadas foram desenvolvidas/configuradas corretamente.
<b>Desenvolvimento de <i>Software</i></b>	Atividade de construção ou parametrização de um <i>software</i> para manutenção ou atualização do mesmo.
<b>Documento de Oficialização de Demanda - DOD</b>	Documento que contém o detalhamento da necessidade da Unidade de Gestão Requisitante da Solução.
<b>Escopo do produto</b>	Descrição detalhada do objetivo do produto.
<b>Parametrização</b>	É a ação de estabelecer parâmetros de processamento de um determinado sistema a fim de atender necessidades específicas.
<b>Partes interessadas</b>	Envolvidos que de alguma forma afetam ou são afetados, positiva ou negativamente, pela demanda.

Termo	Descrição
<b>PDTI</b>	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
<b>Plataforma de aplicação</b>	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 ( <i>desktop</i> , ou <i>web</i> , por exemplo) de como a aplicação será oferecida ao requisitante.
<b>Release</b>	É a entrega de um ou mais Incrementos do Produto prontos, gerados pela Equipe de Desenvolvimento, para que sejam utilizados.
<b>Requisitos básicos</b>	Requisitos básicos necessários para o atendimento da demanda, normalmente relacionados a questões de negócio, de recursos humanos, de desempenho, legais, sociais, ambientais e culturais.
<b>Requisitos de infraestrutura</b>	Requisitos de infraestrutura para a implantação da solução de <i>software</i> .
<b>Requisitos de sustentação</b>	Requisitos para a execução do monitoramento e do suporte do sistema.
<b>Requisitos funcionais</b>	Requisitos relacionados as funcionalidades e serviços do sistema para o atendimento da demanda.
<b>Requisitos não-funcionais</b>	Requisitos relacionados às propriedades e restrições do sistema, como segurança, desempenho, espaço em disco, etc.
<b>Sessão de usuário</b>	Serviço do sistema que possibilita temporariamente o acesso do usuário às funcionalidades do sistema.

## 5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
<b>Resolução CGPAR nº 11 de 10/05/2016</b>	2016	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.
<b>ISO/IEC 27001:2013</b>	2013	<i>Information technology --Security techniques - Information security management systems -- Requirements</i>
<b>ISO/IEC 27002:2013</b>	2013	<i>Information technology --Security techniques --Code of practice for information security controls</i> (Tecnologia da Informação –Técnicas de Segurança – Código de práticas para controles de segurança da Informação)
<b>ISO/IEC 27005:2010</b>	2010	<i>Information technology --Security techniques - Information security risk management</i> (Tecnologia da Informação –Técnicas de Segurança – Gerenciamento Riscos Segurança Informação)
<b>ISO/IEC 27701:2019</b>	2019	<i>Information technology --Security techniques - Privacy Information Management System (PIMS)</i> (Tecnologia da Informação –Técnicas de Segurança –Sistema de Gestao da Privacidade da Informação – SGPI)

## 6. DIRETRIZES

### 6.1. Diretrizes

#	ATIVIDADES
1	<p>Todo e qualquer processo de construção ou de parametrização de <i>software</i> será precedido de planejamento e estar alinhado com a Política de Segurança e Privacidade da SPA vigente. Em complementação, o Instrumento normativo “Gerir Processo de <i>Software</i>” ou outro que o substitua deve ser observado.</p>
2	<p>O ciclo de vida de um <i>software</i> consiste nas seguintes fases:</p> <ul style="list-style-type: none"> <li>○ Recepção de Demandas;</li> <li>○ Definição da Demanda (Escopo e Viabilidade);</li> <li>○ Planejamento da Estratégia de Execução (Plano de Projeto);</li> <li>○ Segurança e Privacidade da Informação (<i>Privacy by Design</i>);</li> <li>○ Realização da Estratégia de Execução;</li> <li>○ Implantação e estabilização; e</li> <li>○ Sustentação e evolução.</li> </ul>

#	ATIVIDADES
3	<p>A Superintendência de Tecnologia da Informação (SUPTI) faz uso de padrões e/ou metodologias para:</p> <ul style="list-style-type: none"> <li>○ Desenvolvimento de sistemas da informação;</li> <li>○ Controles, Segurança e Privacidade das informações;</li> <li>○ Versionamento de código-fonte de sistemas;</li> <li>○ Mensuração do tamanho de <i>software</i>, e;</li> <li>○ Nomenclaturas e documentação de: <ul style="list-style-type: none"> <li>○ arquivos;</li> <li>○ código-fonte, e;</li> <li>○ manuais de procedimentos.</li> </ul> </li> </ul> <p>Estes padrões serão seguidos em todo processo de <i>software</i>.</p>
4	<p>Observar que o processo de <i>software</i> pode ser viabilizado por meio de aquisições de soluções de TI. Neste cenário:</p> <ul style="list-style-type: none"> <li>○ A obrigação dos fornecedores em seguir as práticas de Segurança e Privacidade da Informação definidas na Política;</li> <li>○ Normativos internos de Gestão de compras e contratos, bem como seguir as práticas de Segurança e Privacidade da informação.</li> </ul>
<b>DEFINIÇÃO DE DEMANDA: ESCOPO E VIABILIDADE</b>	
5	<p>Executar as seguintes atividades para definição dos requisitos de <i>software</i>:</p> <ul style="list-style-type: none"> <li>○ Definição da visão de <i>software</i> (escopo e requisitos);</li> <li>○ Controles, Segurança e Privacidade das Informações;</li> <li>○ Análise do processo de negócio, e;</li> <li>○ Estimativa inicial do tamanho de <i>software</i>.</li> </ul>
<b>PLANEJAMENTO DA ESTRATÉGIA DE EXECUÇÃO: PLANO DE PROJETO</b>	
6	<p>As seguintes atividades serão executadas nessa fase:</p> <ul style="list-style-type: none"> <li>○ Escolher a estratégia de execução do projeto;</li> <li>○ Definir a metodologia de desenvolvimento, mais adequada para a solução de <i>software</i>, sendo recomendada a utilização de uma metodologia ágil;</li> <li>○ Implementar os Controles de Proteção e Privacidade de dados;</li> <li>○ Planejar os testes a serem realizados;</li> <li>○ Planejar o monitoramento do projeto;</li> <li>○ Planejar a carga de dados, quando couber;</li> <li>○ Planejar os manuais e treinamentos necessários;</li> <li>○ Definir a arquitetura preliminar do <i>software</i>;</li> <li>○ Verificar a infraestrutura disponível para o funcionamento do <i>software</i> e planejar atualizações;</li> <li>○ Planejar a sustentação adequada para manter o <i>software</i>, e;</li> <li>○ Planejar o desenvolvimento do <i>software</i>.</li> </ul>

#	ATIVIDADES
<b>DESENVOLVIMENTO DE SOFTWARE</b>	
7	<p>Considerar aspectos pela SUPTI de Segurança e privacidade da Informação nestas atividades:</p> <ul style="list-style-type: none"> <li>○ Preparação dos ambientes;</li> <li>○ Execução do desenvolvimento, quando couber;</li> <li>○ Execução dos testes e documentação dos resultados;</li> <li>○ Gerenciamento de aquisições, caso existam;</li> <li>○ Documentação do desenvolvimento realizado;</li> <li>○ Planejamento da implantação;</li> <li>○ Planejamento de treinamentos e elaboração de manuais;</li> <li>○ Homologação do sistema;</li> <li>○ Medição do tamanho final do software;</li> <li>○ Planejamento da implantação, e;</li> <li>○ Treinamentos.</li> </ul>
<b>DESENVOLVIMENTO TERCEIRIZADO</b>	
8	<p>As seguintes atividades serão realizadas pela SUPTI quando do desenvolvimento terceirizado:</p> <ul style="list-style-type: none"> <li>○ Acordo de licença, propriedade do código e direitos de propriedade intelectual apropriados;</li> <li>○ Requisitos contratuais para um projeto seguro, práticas de código e testes;</li> <li>○ Fornecimento de um modelo de ameaça aprovado para o desenvolvedor externo;</li> <li>○ Teste de aceitação relativos à qualidade e exatidão dos itens entregues;</li> <li>○ 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;</li> <li>○ Acordos de garantia para o caso do código fonte não estiver mais disponível;</li> <li>○ Direitos autorais para auditar os controles e processos de desenvolvimento.</li> </ul>
9	<p>Aspectos de Segurança e Privacidade de dados serão considerados nos ambientes de:</p> <ul style="list-style-type: none"> <li>○ Desenvolvimento;</li> <li>○ Homologação e Testes e;</li> <li>○ Produção.</li> </ul>
<b>GESTÃO DE MUDANÇAS</b>	

#	ATIVIDADES
10	<p>As seguintes atividades serão consideradas:</p> <ul style="list-style-type: none"> <li>○ Manutenção de registros para níveis acordados de autorização;</li> <li>○ Garantia de que as mudanças sejam submetidas apenas por usuários autorizados;</li> <li>○ Identificação de todo <i>software</i>, informação, entidades em bancos de dados e <i>hardware</i> que precisem de correções;</li> <li>○ Aprovação formal para propostas antes dos inícios dos trabalhos;</li> <li>○ Garantia de que os usuários autorizados aceitem as mudanças antes da implementação;</li> <li>○ Garantia da atualização da documentação do sistema após a conclusão de cada mudança, bem como manutenção da documentação antiga;</li> <li>○ Controle de versão para atualização de <i>software</i>;</li> <li>○ Trilha de auditoria para todas as mudanças autorizadas;</li> <li>○ Horários apropriados para implementação de mudanças, de modo a não perturbar os processos de negócio envolvidos.</li> </ul>
11	<p>Aspectos de Segurança e Privacidade de dados serão considerados nas seguintes atividades de documentação produzida para o sistema finalizado:</p> <ul style="list-style-type: none"> <li>○ ter suas versões controladas, e:</li> <li>○ ter informações suficientes para permitir: <ul style="list-style-type: none"> <li>○ sua instalação;</li> <li>○ sua operação;</li> <li>○ seu uso, e;</li> <li>○ sua manutenção.</li> </ul> </li> <li>○ Testes de Segurança do Sistema;</li> <li>○ Testes de Aceitação do Sistema.</li> </ul>
<b>DADOS PARA TESTES</b>	
12	<p>As seguintes atividades serão consideradas:</p> <ul style="list-style-type: none"> <li>○ Aplicar nos dados de teste os mesmos procedimentos de controle de acesso aplicados em sistemas de aplicações operacionais;</li> <li>○ A cada teste deve ser obtida autorização para utilizar uma cópia da informação operacional;</li> <li>○ Após finalizar os testes, deve ser apagada a informação operacional;</li> <li>○ Registrar, para fins de trilha de auditoria, que uma cópia da informação operacional foi utilizada para testes.</li> </ul>
<b>IMPLANTAÇÃO E ESTABILIZAÇÃO DE SOFTWARE</b>	

#	ATIVIDADES
13	<p>As seguintes atividades serão executadas durante a implantação e estabilização de <i>software</i>:</p> <ul style="list-style-type: none"> <li>○ Planejamento do tratamento de incidentes de Segurança da Informação;</li> <li>○ Preparação do ambiente de produção;</li> <li>○ Execução da implantação;</li> <li>○ Monitoramento da implantação;</li> <li>○ Gerenciamento das aquisições, e;</li> <li>○ Realização das cargas de dados, quando couber.</li> </ul>
<b>MONITORAMENTO E CONTROLE</b>	
14	<p>Esta fase contém as seguintes atividades:</p> <ul style="list-style-type: none"> <li>○ Manutenção da Qualidade;</li> <li>○ Revisão de escopo e requisitos;</li> <li>○ Gerenciamento de Riscos de Segurança e Privacidade de Dados.</li> </ul>
<b>CONTROLE DE ACESSO</b>	
15	<p>Serão consideradas as diretrizes definidas no Instrumento Normativo de Processo “INP-SUPTI-TIC-140-009-Gestao de Acesso” de modo que as funcionalidades desenvolvidas em um <i>software</i> sejam acessadas apenas por pessoal com autorização para tal.</p>
<b>CLASSIFICAÇÃO DA INFORMAÇÃO</b>	
16	<p>As seguintes atividades serão realizadas quanto a classificação da informação no processo de aquisição, desenvolvimento e manutenção de <i>software</i>:</p> <ul style="list-style-type: none"> <li>○ Mascaram dados para todo dado classificado como confidencial, de acordo com as diretrizes de Classificação da Informação, limitando a exposição deste tipo de dado para usuários sem privilégios;</li> <li>○ Classificar como confidencial os dados de <i>logs</i> de acesso e de transações.</li> </ul>

## 6.2. Consenso / Aprovação

Este Instrumento Normativo deve ser aprovado pela Diretoria Executiva.

## 7. PAPÉIS E RESPONSABILIDADES

### 7.1. Da Unidade Responsável

Área	Atividades	Ferramenta
Gerência de Desenvolvimento de Sistemas (GEDES)	Responsável pelo ciclo de vida de sistemas utilizados na SPA.	N/A

## 7.2. Das Unidades Executoras

Área	Atividades	Ferramenta
Segurança da Informação	Garantir a Segurança na execução dos projetos.	N/A

## 8. DISPOSIÇÕES FINAIS

Os casos omissos ou excepcionais neste Instrumento Normativo serão submetidos à análise e aprovação da Diretoria Executiva.

A não observância aos dispositivos desse documento pode acarretar, nos termos da legislação e normativos internos aplicáveis, sanções administrativas, civis e/ou penais.

## 9. ANEXOS

N/A

Registro de Alterações				
Tópico	Versão	Página	Data	Descrição Sumária