<table>
<tr><td rowspan="4"></td><td colspan="4">SANTOS PORT AUTHORITY</td></tr>
<tr><td colspan="3">Instrumento Normativo de Processo</td><td>Código: TIC-140-019</td></tr>
<tr><td colspan="2">Diretoria Responsável:
Presidência</td><td colspan="2">Unidade Responsável:
Gerência de Desenvolvimento de Sistemas</td><td>Elaboração:
Supervisão de Governança de TI</td></tr>
<tr><td>Início da vigência:
05/11/2021</td><td>Próxima revisão:
05/11/2023</td><td>Aprovação:
Resolução DIPRE nº 466.2021</td><td>Validação:
Superintendência de Tecnologia da Informação</td></tr>
<tr><td colspan="4">Assunto:
Sistema de Gestão da Privacidade da Informação: Privacidade por Desenho e por Padrão, Anonimização e Pseudominização</td><td>Versão: 1.1</td></tr>
</table>

Instrumento Normativo de Processo - Sistema de Gestão da Privacidade da Informação: Privacidade por Desenho e por Padrão, Anonimização e Pseudominização

SUMÁRIO

1. OBJETIVO **3**

2. ABRANGÊNCIA **3**

3. FUNDAMENTAÇÃO **3**

4. DEFINIÇÕES **3**

5. ARCABOUÇO LEGAL **4**

6. DIRETRIZES **5**

6.1. Diretrizes ***5***

6.2. Consenso / Aprovação ***6***

7. PAPÉIS E RESPONSABILIDADES **6**

7.1. Da Unidade Responsável ***6***

7.2. Das Unidades Executoras ***7***

8. DISPOSIÇÕES FINAIS **7**

9. ANEXOS **7**

1. OBJETIVO

Estabelecer as diretrizes que assegurem que processos e sistemas sejam projetados de forma que a coleta e o tratamento de Dados Pessoais (incluindo o uso, divulgação, retenção, transmissão, descarte, compartilhamento, transferência e divulgação) estejam limitados ao que é necessário para o propósito identificado.

2. ABRANGÊNCIA

Todos os sistemas corporativos que são utilizados em ambientes de produção na *Santos Port Authority* – SPA, e se aplica a Diretoria Executiva, 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 da Informação da SPA, em vigor.

4. DEFINIÇÕES

Termo	Descrição
Privacidade por Desenho ***(Privacy by Design)***	É uma abordagem a qual leva em conta a privacidade durante todo o processo de construção de um software ou serviço, considerando os seguintes princípios: • Pró-ativo não reativo; preventivo não corretivo, de modo a evitar incidentes de violação à privacidade; • Privacidade como configuração padrão: as configurações padrão de determinado sistema devem ser ajustadas desde o início para preservar a privacidade do usuário; • Privacidade incorporada ao *design*, incluindo a arquitetura e modelos de negócio; • Funcionalidade total - soma positiva, não soma zero; • Segurança de ponta a ponta: proteção completa incorporada ao ciclo de vida da informação; • Visibilidade e transparência - mantê-lo aberto; • Respeito pela privacidade do usuário: mantê-lo centrado nos interesses do usuário. Fonte: https://pt.wikipedia.org/wiki/Privacidade_desde_a_concepção

Termo	Descrição
Privacidade por Padrão ***(Privacy by Default)***	Diz respeito à adoção da proteção de dados pessoais como padrão em todos os processos e atividades desenvolvidos pela empresa, por meio da definição de medidas de segurança, técnicas e organizacionais que devem ser aplicadas de forma padronizada e constante, em todas as áreas, projetos, produtos. Inclusive verificando se o mínimo necessário em termos de proteção de dados está sendo observado, como finalidade específica e legítima para o tratamento de dados pessoais, ou a minimização dos dados sempre que aplicável. Fonte: https://www.infranewstelecom.com.br/entenda-as-diferencas-entre-privacy-by-design-e-privacy-by-default/
Minimização	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Fonte:https://www.conjur.com.br/2021-jun-15/lara-impacto-positivo-minimizacao-coleta-dados-pessoais
Anonimização	Técnica que através da "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" e que resulte em dado anonimizado (dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento). Fonte: Lei nº 13.709, Art 5º, incisos III e XI.
Pseudonimização	É 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. Fonte: Lei nº 13.709, Art 13º, §4º.
Arquivos Temporários	Arquivos criados como resultado de tratamento de dados pessoais, específicos de um sistema ou aplicação ou banco de dados (inclusive para *rollback* de transações).

5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
Lei nº 13.709	2018	Lei Geral de Proteção de Dados Pessoais (LGPD).

ISO/IEC 27001:2013	2013	*Information technology -- Security techniques - Information security management systems -- Requirements*
ISO/IEC 27002:2013	2013	*Information technology -- Security techniques -- Code of practice for information security controls* (Tecnologia da Informação – Técnicas de Segurança – Código de práticas para controles de segurança da Informação)
ISO/IEC 27701:2019	2019	*Information technology -- Security techniques - Privacy Information Management System (PIMS)* (Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestao da Privacidade da Informação – SGPI)

6. DIRETRIZES

6.1. Diretrizes

#	ATIVIDADES
PRIVACIDADE POR DESENHO E POR PADRÃO	
1	Deve-se limitar a coleta e o tratamento de dados pessoais ao mínimo que seja relevante, proporcional e necessário para a finalidade a que se destina. Cabe os princípios da privacidade por desenho e por padrão.
2	Onde existir opção de escolha pelo titular, relativo à coleta e/ou tratamento de dados pessoais, que essa opção seja desabilitada por padrão e somente habilitada mediante escolha explicita do titular de Dados Pessoais.
3	Deve-se adotar procedimentos para assegurar que os dados pessoais, são precisos, completos e atualizados de acordo com as finalidades os quais são tratados durante o ciclo de vida do dado pessoal.
4	Deve-se adotar em seus processos de coleta de dados pessoais, a minimização, e quando desnecessário a identificação dos titulares a anonimização ou a pseudonimização.
5	Ao final do tratamento, resguardado os requisitos legais pertinentes, deve-se adotar procedimentos para excluir os dados pessoais ou anonimize-os de forma a não possibilitar a identificação e/ou reidentificação, considerando que os dados pessoais não são mais necessários.
6	Arquivos temporários contendo dados pessoais devem ser descartados.

#	ATIVIDADES
7	Dados pessoais não devem ser retidos por um período além do necessário, de acordo com as finalidades para os quais são tratados.
8	Considerar o descarte de dados pessoais, conforme INP-SUPTI-TIC-140-014- Aquisição, Desenvolvimento e Manutenção de Software.
9	Considerar o controle de transmissão de dados pessoais, conforme "INP-SUPTI-TIC-140-013-Segurança nas Comunicações", observando-se controles pertinentes.
COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO DE DADOS PESSOAIS	
10	A transferência de dados pessoais entre jurisdições (nacionais e/ou internacionais) deve ser realizada, quando aplicável, documentada e resguardada por legislações e/ou regulamentações. O *compliance* com estes requisitos devem ser documentados, inclusive países e organizações internacionais para o quais os dados pessoais possam ser transferidos.
11	A transferência de dados pessoais quando executada deve ser registrada e a cooperação com estes terceiros, seja assegurada para apoiar o cumprimento de obrigações para os titulares.
12	A divulgação de dados pessoais, durante o curso normal do tratamento, deve ser registrada incluindo quais dados foram divulgados. Adicionalmente divulgações resultantes de investigações legais e/ou auditoria externas, também devem ser registradas.

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 processos.	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**