<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-140-011</td></tr>
<tr><td colspan="2">Diretoria Responsável: Presidência</td><td>Unidade Responsável: Superintendência de Tecnologia da Informação</td><td>Elaboração: Supervisão de Governança de TI</td></tr>
<tr><td>Início da vigência: 30/06/2021</td><td>Próxima revisão: 30/06/2023</td><td>Aprovação: Decisão Direxe nº 265.2021</td><td>Validação: Superintendência de Tecnologia da Informação</td></tr>
<tr><td colspan="3">Processo: Sistema de Gestão da Privacidade da Informação: Segurança Física e Ambiente</td><td>Versão: 1.1</td></tr>
</table>

Instrumento Normativo de Processo Sistema de Gestão da Privacidade da Informação: Segurança Física e Ambiente

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 8

7. PAPÉIS E RESPONSABILIDADES 8

7.1. Da Unidade Responsável 8

7.2. Das Unidades Executoras 9

8. DISPOSIÇÕES FINAIS 9

9. ANEXOS 9

1. OBJETIVO

Estabelecer as diretrizes para prevenir o acesso físico não autorizado, danos ou interferência às instalações físicas e aos ativos de tecnologia da informação e às informações da Companhia.

2. ABRANGÊNCIA

Todos os ambientes físicos da SPA que possuem recursos de Tecnologia da Informação que geram, processam, armazenam e/ou transmitem dados, a todos os usuários, inclusive clientes e fornecedores da SPA que se utilizem de recursos físicos ou de Redes para acesso às informações.

3. FUNDAMENTAÇÃO

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

4. DEFINIÇÕES

Termo	Descrição
Áreas Seguras de TI	Espaços físicos que precisam de proteção contra as ameaças, que poderiam gerar um incidente de segurança da informação, por isso a SPA criou e mantém perímetros de segurança e controles para proteger seus ativos de informação, conforme sua criticidade.
ANS (Acordo de Nível de Serviço)	Acordo firmado entre a área de TI e as áreas de negócios da Companhia que utilizam os serviços de TI. Este acordo descreve os serviços de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo.

Termo	Descrição
Mesa Limpa/Tela Limpa	Mesa limpa e tela limpa se refere a práticas relacionadas de segurança da informação para assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., *notebooks*, celulares, *tablets*, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período de tempo ou ao final do dia.
Usuário	Todos os empregados, estagiários, menores aprendizes, terceirizados, que possuem acesso aos ativos de TI e de negócio disponibilizados pela SPA.

5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
Resolução CGPAR nº 11 de 10/05/2016	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.
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 27005:2010	2010	*Information technology --Security techniques - Information security risk management* (Tecnologia da Informação –Técnicas de Segurança – Gerenciamento Riscos Segurança 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 Privacidadeda Informação – SGPI)

6. DIRETRIZES

6.1. Diretrizes

#	ATIVIDADES
1	As áreas seguras de TI da SPA são definidas pela SUPTI e sua definição leva em consideração: • Perímetro; • Controles de entrada e saída; • Salas e outras instalações que não o Data Center.
2	O acesso às áreas seguras de TI da SPA é restrito aos empregados autorizados formalmente pela SUPTI, para desempenho de suas atividades.
3	Revisar periodicamente a lista de empregados definidas pela SUPTI, com acesso classificado como sigilosa.
4	São considerados Incidentes de Segurança quando ocorre em áreas seguras: • Acesso indevido, não autorizado; • Abertura, manuseio ou manutenção de ativos de TI sem autorização.

#	ATIVIDADES

5	Incidentes em áreas seguras considerar:
	• Fenômenos naturais;
	• Ações de vandalismo;
	• Qualquer evento de ordem social que gerar risco potencial de indisponibilidade de dados e sistemas ou destruição da área segura.
	• Sistemas de:
	  ○ Cópias de segurança para os dados processados na área;
	  ○ Detecção, alertas e extintores de incêndio;
	  ○ Controles de unidade e temperatura.

6	É terminantemente proibido em áreas seguras de TI: • Fumar; • Beber; • Comer; • Documentos impressos; • Produtos inflamáveis; • Qualquer outra atividade que não esteja especificamente vinculada com as atividades de operação e manutenção dos ativos de tecnologia da informação.
7	A limpeza e conservação de áreas seguras de TI será realizada: • Apenas por profissionais cadastrados e autorizados pela SUPTI; • Utilizando-se produtos de limpeza específicos para o ambiente.

#	ATIVIDADES

8	Considerar durante o ciclo de vida dos Ativos e recursos de Tecnologia da Informação:
	• Instalação e Proteção:
	  ○ Contra falta de energia elétrica e variação de temperatura/umidade;
	  ○ Local, considerando risco de quedas ou danos de qualquer natureza;
	  ○ Trancas ou cadeados para impedir acesso indevido ao conteúdo;
	  ○ Proteção de cabeamento contra interferências, intervenções ou ataques intencionais que resultem em interrupção de comunicação.
	• Manutenção:
	  ○ Contrato de Manutenção Preventiva para ativos com risco de indisponibilidade igual ou superior a médio.
	• Reutilização e descarte:
	  ○ Considerar os instrumentos INP-SUPTI-TIC-140-012-Segurança nas Operações e INP-SUPTI-TIC-140-013-Segurança nas Comunicações.

9	Segurança de equipamentos e ativos fora das dependências da SPA • Supervisionados quando em lugares públicos; • Seguindo as normas do fabricante para a devida proteção do equipamento ou políticas de proteção e classificação para informações; • Avaliação de Riscos para *Home Office* ou Tele trabalho; • Registros quando transferidos entre pessoas e/ou locais.

#	ATIVIDADES
10	Considerar: • Mesa limpa; • Tela limpa. Será adotada pelos empregados uma política de mesa limpa e tela limpa, que consiste da proteção contra perdas, roubo ou furto de informações sensíveis. As seguintes práticas serão adotadas: • Manter seu local de trabalho, limpo e organizado; • Manter organizados documentos e mídias necessários às atividades do dia-a-dia, protegidos em pastas, dentro de armários ou gavetas, a fim de evitar que sejam danificadas, destruídas ou mesmo furtadas; • Não expor informações sensíveis, sigilosas, confidenciais ou restritas, tais como: relatórios, propostas comerciais, contratos, dados de clientes, mídias, etc. Armazenar informações sensíveis, sigilosas, confidenciais ou restritas, em local seguro, trancado com chaves ou cadeado e protegido de acesso não autorizado ou indevido.

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
SUPTI	Identificação, escolha, implantação e manutenção dos controles tecnológicos que apoiam a proteção das áreas, ambientes e ativos de informação em todos os departamentos dentro da SPA.	N/A

7.2. Das Unidades Executoras

Área	Atividades	Ferramenta
GERID	Controlar acesso às áreas seguras.	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.

<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-140-011</td></tr>
<tr><td>Diretoria Responsável: Presidência</td><td colspan="2">Unidade Responsável: Superintendência de Tecnologia da Informação</td><td>Elaboração: Supervisão de Governança de TI</td></tr>
<tr><td>Início da vigência: 30/06/2021</td><td>Próxima revisão: 30/06/2023</td><td>Aprovação: Decisão Direxe nº 265.2021</td><td>Validação: Superintendência de Tecnologia da Informação</td></tr>
<tr><td colspan="3">Processo: Sistema de Gestão da Privacidade da Informação: Segurança Física e Ambiente</td><td>Versão: 1.1</td></tr>
</table>

Registro de Alterações				
Tópico	**Versão**	**Página**	**Data**	**Descrição Sumária**