<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-140-013</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: 05/08/2021</td><td>Próxima revisão: 05/08/2023</td><td>Aprovação: Decisão Direxe nº 319.2021</td><td>Validação: Superintendente de Tecnologia da Informação</td></tr>
<tr><td colspan="3">Processo: Sistema de Gestão da Privacidade da Informação: Segurança nas Comunicações</td><td>Versão: 1.1</td></tr>
</table>

Instrumento Normativo de Processo

Sistema de Gestão da Privacidade da Informação

Segurança nas Comunicações

SUMÁRIO

1. OBJETIVO 3

2. ABRANGÊNCIA 3

3. FUNDAMENTAÇÃO 3

4. DEFINIÇÕES 3

5. ARCABOUÇO LEGAL 4

6. DIRETRIZES 4

6.1. Diretrizes 4

6.2. Consenso / Aprovação 7

7. PAPÉIS E RESPONSABILIDADES 8

7.1. Da Unidade Responsável 8

8. DISPOSIÇÕES FINAIS 8

9. ANEXOS 8

1. OBJETIVO

Assegurar a proteção das informações em redes e dos recursos de processamento de dados que as apoiam.

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
Redes públicas	Redes caracterizadas pelo acesso ao público em geral de forma indistinta disponíveis em locais públicos, como *cyber*-cafés, shoppings, etc. Também são redes constituídas por entes públicos, como instituições de ensino público, pesquisas governamentais, etc. Para o presente Instrumento considera-se o primeiro significado.

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

#	Diretrizes
1	A SUPTI é responsável pelo gerenciamento e controle das redes para proteger as informações nos sistemas e aplicações da SPA.

#	Diretrizes
2	A SUPTI deve estabelecer e manter controles, bem como elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) para as funções abaixo: ○ Estabelecer funções, responsabilidades e procedimentos para gerenciar os ativos de rede; ○ Se possível, separar a responsabilidade operacional das redes da operação dos recursos computacionais; ○ Estabelecer controles para a proteção da confidencialidade e integridade dos dados que trafegam nas redes internas, públicas e sem fio, bem como sistemas e aplicações a elas conectadas; ○ Estabelecer controles para manter a disponibilidade dos serviços e dispositivos de processamento de dados conectados; ○ Estabelecer mecanismos de autenticação para todos os sistemas que trafegam nas redes; ○ Restringir por meios de direito de acesso todas as conexões à rede.
SEGURANÇA PARA OS SERVIÇOS DE REDE	
3	A SUPTI deve aplicar tecnologias para a segurança dos serviços de redes tais como autenticação, criptografia e controles de conexão de rede.
4	A SUPTI é responsável por ativar e manter parâmetros técnicos para conexões seguras com serviços de rede de acordo com regras de segurança para conexão com redes.
SEGREGAÇÃO E REDES	
5	A SUPTI deve manter segregados grupos de serviços de informação, usuários e sistemas de informação, bem como áreas de desenvolvimento, de testes e de produção.
TRANSFERÊNCIA DE INFORMAÇÕES ATRAVÉS DE REDES	

#	Diretrizes
6	A SUPTI quando da transferência de Informações através de redes: ○ Protegerá a informação transferida contra interceptação, cópia, modificação, desvio ou destruição; ○ Detectará e protegerá a informação contra código malicioso que possa ser transferido através da rede; ○ Protegerá informações classificadas como sigilosas que sejam transmitidas através de anexos de e-mail; ○ Especificará o uso aceitável dos recursos de comunicação de dados; ○ Evitará comprometer a SPA, através de seus empregados e fornecedores, de difamação, assédio, falsa identidade, retransmissão de “correntes” e notícias falsas, compras não autorizadas etc.; ○ Fará uso de criptografia para proteger as informações classificadas como sigilosas transmitidas através das redes; ○ Controlará a retransmissão automática de mensagens eletrônicas para endereços externos; ○ Orientará os empregados e terceiros, por meio de treinamentos, comunicações, na adoção de precauções apropriadas para não revelar informações classificadas como sigilosas.
7	A SUPTI, quando de acordos para transferência de informações, elaborará Procedimentos Operacionais Padrão (POP) ou Manuais, quando aplicável, para: ○ Responsabilizar os gestores pelo controle e notificação de transmissões, expedições e recepções; ○ Garantir a rastreabilidade e o não repudio dos eventos; ○ Elaborar padrões e práticas para embalagem e transmissão de informações; ○ Elaborar acordos para procedimentos de custódia; ○ Proceder à identificação de portadores; ○ Determinar funções, papéis e responsabilidades na ocorrência de incidentes de segurança da informação; ○ Utilizar um sistema acordado para identificar informações sensíveis e sigilosas garantindo que o significado dos rótulos seja imediatamente entendido, e que esta informação seja ou esteja devidamente protegida; ○ Fazer uso de criptografia para proteção de informações classificadas como sigilosas; ○ Manter uma cadeia de custódia para informações em trânsito.

MENSAGENS EM FORMATO ELETRÔNICO	
8	A SUPTI: ○ Protegerá as mensagens contra: acesso não autorizado, modificação, negação de serviço, de acordo com o esquema de classificação da SPA; ○ Garantirá que o endereço de destino e o meio de transporte de mensagens estejam corretos; ○ Manterá o serviço disponível e confiável; ○ Criará e manterá requisitos de assinatura eletrônica para aspectos legais; ○ Aprovará previamente o uso de serviços públicos externos tais como mensagens instantâneas e de compartilhamento de arquivos; ○ Manterá níveis mais altos de autenticação para acesso a partir de redes públicas.
ACORDOS DE CONFIDENCIALIDADE E DE NÃO DIVULGAÇÃO	
9	A SUPTI: ○ Definirá quais informações devem ser protegidas e como serão protegidas; ○ Definirá a duração esperada de um acordo, incluindo situações em que a confidencialidade tenha de ser mantida indefinidamente; ○ Definirá quais ações devem ser executadas ao fim de um acordo; ○ Definirá as responsabilidades dos signatários do acordo para evitar a divulgação não autorizada da informação; ○ Relacionará a proteção da informação sigilosa com o proprietário da informação, com segredos comerciais e com a propriedade intelectual; ○ Definirá os direitos do signatário de acordo para fazer uso de uma informação sigilosa; ○ Auditará e irá monitorar as atividades que envolvem informações sigilosas; ○ Criará e manterá um procedimento para notificar e reportar a divulgação não autorizada ou o vazamento de informações sigilosas; ○ Criará, implementará e manterá regras para retomar ou destruir uma informação ao fim do acordo; ○ Criará e implementará ações e penalidades a serem tomadas no vaso de violação do acordo.

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	Aplicação das políticas e práticas de Segurança da Informação. Responsável pelos controles tecnológicos que apoiam a proteção da informação de todas as Unidades de Gestão da SPA, nos aspectos de: • Identificação; • apresentação; • sustentação; • escolha; • implantação; e, • manutenção.	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**