

	SANTOS PORT AUTHORITY			
	Instrumento Normativo de Processo			Código: TIC-140-010
	Diretoria Responsável: Presidência	Unidade Responsável: Superintendência de Tecnologia da Informação		Elaboração: Supervisão de Governança de TI
	Início da vigência: 05/08/2021	Próxima revisão: 05/08/2023	Aprovação Decisão Direxe nº 320.2021	Validação: Superintendente de Tecnologia da Informação
Processo: Sistema de Gestão da Privacidade da Informação: Criptografia				Versão: 1.1

Instrumento Normativo de Processo

Sistema de Gestão da Privacidade da Informação: Criptografia

SUMÁRIO

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

1. OBJETIVO

Estabelecer as atividades para aplicação de processos criptográficos sobre informações classificadas de acordo com a tabela de classificação da informação no âmbito da responsabilidade da SPA, visando assegurar que as informações recebam um nível adequado de proteção.

2. ABRANGÊNCIA

Todos os tipos de informações classificadas de acordo com a tabela de classificação da informação, e de acordo com a Tabela de Classificação de Ativos disponível na Política de Segurança, Privacidade e SGPI da SPA, e se aplicam a todos os empregados, os cedidos, os estagiários e os terceirizados que executam atividades nas instalações da Companhia.

3. FUNDAMENTAÇÃO

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

4. DEFINIÇÕES

Termo	Descrição
Criptografia	Procedimento para garantir, através de codificação do próprio dado, que apenas quem tiver conhecimento do mecanismo de decodificação, terá acesso ao mesmo.
Chave pública	Criptografia de chave pública, também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que podem ser amplamente disseminadas. Em um sistema de criptografia de chave pública, qualquer pessoa pode criptografar uma mensagem usando a chave pública do destinatário.
Chave privada	Também chamada de criptografia de chave simétrica, secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.
Certificado Digital	Assinatura digital que garante agilidade e segurança nas transações eletrônica de dados.

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	<i>Information technology --Security techniques - Information security management systems -- Requirements</i>
ISO/IEC 27002:2013	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)
ISO/IEC 27005:2010	2010	<i>Information technology --Security techniques - Information security risk management</i> (Tecnologia da Informação –Técnicas de Segurança – Gerenciamento Riscos Segurança Informação)
ISO/IEC 27701:2019	2019	<i>Information technology --Security techniques - Privacy Information Management System (PIMS)</i> (Tecnologia da Informação –Técnicas de Segurança –Sistema de Gestão da Privacidade da Informação – SGPI)

6. DIRETRIZES

6.1. Diretrizes

#	ATIVIDADES
1	Informações classificadas de acordo com a tabela de classificação da informação serão armazenadas e transmitidas de forma criptografada, tanto por <i>hardware</i> como por <i>software</i> .
2	Informações pessoais classificadas como sensíveis pela LGPD serão armazenadas e transmitidas de forma criptografada por <i>hardware</i> ou por <i>software</i> .
3	A Gerência de Carreira e Capacitação (GECAR) em conjunto com a SUPTI promoverá treinamentos visando capacitar os empregados na atividade de criptografia, bem como instruí-los na atividade de classificação de uma informação.
4	Quando da utilização de criptografia de chave pública, caberá exclusivamente à SUPTI o gerenciamento e proteção das chaves privadas.

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	Gerenciamento das chaves públicas de criptografia.	N/A
<i>Security Officer</i> (RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO)	Empregado oficialmente nomeado e responsável pela manutenção do Sistema de Gestão da Privacidade da Informação (SGPI).	N/A

7.2. Das Unidades Executoras

Área	Atividades	Ferramenta
Gerência de Carreira e Capacitação (GECAR)	Treinamento na utilização de criptografia.	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