# POLÍTICA DE SEGURANÇA E PRIVACIDADE, E SISTEMA DE GESTÃO DE PRIVACIDADE DA INFORMAÇÃO – SGPI

# SUMÁRIO

CAPÍTULO I – DISPOSIÇÕES INICIAIS ..... 4

SEÇÃO I – OBJETIVOS DA POLÍTICA ..... 4

12. DECLARAÇÃO DE COMPROMISSO DA ALTA GESTÃO ..... 6

13. ESTRUTURA ORGANIZACIONAL ..... 6

SEÇÃO II – ABRANGÊNCIA ..... 8

SEÇÃO III – FUNDAMENTAÇÃO LEGAL E NORMATIVA ..... 8

SEÇÃO IV – DEFINIÇÕES ..... 10

CAPÍTULO II – PRINCÍPIOS ..... 11

CAPÍTULO III – DIRETRIZES ..... 11

SEÇÃO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE ..... 11

18. OBJETIVOS ESPECÍFICOS ..... 11

19. CLASSIFICAÇÃO DA INFORMAÇÃO ..... 12

19.1. CRITÉRIOS DE CLASSIFICAÇÃO ..... 12

20. REQUISITOS GERAIS DE MANIPULAÇÃO DAS INFORMAÇÕES ..... 15

21. CONSIDERAÇÕES GERAIS ..... 16

SEÇÃO II – TRATAMENTO E PROTEÇÃO DOS DADOS PESSOAIS ..... 17

22. CONSIDERAÇÕES ..... 17

22.1. DIREITOS DO EMPREGADO ..... 17

22.2. DEVER DE NÃO FORNECER DADOS DE TERCEIROS ..... 19

22.3. INFORMAÇÕES COLETADAS ..... 19

22.4. TIPOS DE DADOS COLETADOS ..... 19

22.5. FUNDAMENTO JURÍDICO PARA O TRATAMENTO DOS DADOS PESSOAIS ..... 21

22.6. FINALIDADES DO TRATAMENTO DOS DADOS PESSOAIS ..... 22

22.7. PRAZO DE CONSERVAÇÃO DOS DADOS PESSOAIS ..... 23

22.8. DESTINATÁRIOS E TRANSFERÊNCIA DOS DADOS PESSOAIS ..... 24

22.9. DO TRATAMENTO DOS DADOS PESSOAIS ..... 24

22.9.1. DO RESPONSÁVEL PELO TRATAMENTO DOS DADOS (DATA CONTROLLER) 24

22.9.2. SEGURANÇA NO TRATAMENTO DOS DADOS PESSOAIS DO EMPREGADO ..25

22.9.3. DADOS DE NAVEGAÇÃO (COOKIES) ..... 26

22.9.4. COOKIES DA INTRANET DA SPA ..... 27

22.9.5. GESTÃO DOS COOKIES E CONFIGURAÇÕES DO NAVEGADOR ..... 27
22.10. RECLAMAÇÃO A UMA AUTORIDADE DE CONTROLE ..... 28
23. DAS ALTERAÇÕES ..... 28
24. DO DIREITO APLICÁVEL E DO FORO ..... 29
25. CONTROLES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE ..... 29
26. IMPLANTAÇÃO E AVALIAÇÃO ..... 29
27. EXCEÇÃO À POLÍTICA ..... 29
SEÇÃO III – SGPI – SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO .. 30
28. RISCO ..... 30
29. REQUISITOS ..... 31
29.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (ESTE DOCUMENTO) 31
29.2. ORGANIZAÇÃO DA SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO ..... 31
29.3. RECURSOS HUMANOS ..... 31
29.4. GESTÃO DE ATIVOS DE INFORMAÇÃO ..... 31
29.5. CONTROLE DE ACESSO ..... 32
29.6. USO DE CRIPTOGRAFIA ..... 32
29.7. SEGURANÇA FÍSICA DO AMBIENTE DE TRABALHO ..... 32
29.8. SEGURANÇA DAS OPERAÇÕES ..... 32
29.9. SEGURANÇA DAS COMUNICAÇÕES ..... 33
29.10. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS ..... 33
29.11. RELACIONAMENTO COM FORNCEDORES E TERCEIROS ..... 33
29.12. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ..... 34
29.13. GESTÃO DA CONTINUIDADE DO NEGÓCIO ..... 34
29.14. CONFORMIDADE (COMPLIANCE) ..... 34
CAPÍTULO IV – RESPONSABILIDADES ..... 34
CAPÍTULO V – SANÇÕES ..... 38
CAPÍTULO VI – DISPOSIÇÕES GERAIS ..... 38
ANEXO 1 – TERMO DE RESPONSABILIDADE INDIVIDUAL ..... 39
INFORMAÇÕES DE CONTROLE ..... 42

# POLÍTICA DE SEGURANÇA E PRIVACIDADE E SGPI DA AUTORIDADE PORTUÁRIA DE SANTOS S.A.

## CAPÍTULO I – DISPOSIÇÕES INICIAIS

**1.** Fica instituída a Política de Segurança e Privacidade e SGPI da Autoridade Portuária de Santos S.A. (***"Santos Port Authority"***, **"SPA"** ou **"Companhia"**) como parte integrante do conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação e melhoria contínua na estrutura organizacional da Companhia.

### SEÇÃO I – OBJETIVOS DA POLÍTICA

**2.** O Sistema de Gestão de Privacidade da Informação (SGPI) tem como objetivo a mitigação sistemática dos riscos à segurança e à privacidade da informação.

**3.** Os instrumentos normativos e instruções de trabalho derivados desta política são de cumprimento obrigatório, aplicáveis a todos os funcionários (ou empregados), contratados, terceirizados, trabalhadores temporários, ou com acesso a qualquer informação, sistema, computador, rede de computadores, telecomunicação, mensagem ou serviço de informações pertencentes à SPA em todas suas instalações, onde as leis locais, estatutos e regulamentações do governo não se sobreponham a essas políticas e procedimentos e de acordo com o escopo definido.

**4.** A SPA entende que a Informação, desde sua criação e processamento até seu descarte, é um componente indispensável no processo de tomada de decisão dos gestores, com o objetivo de dar cumprimento à Missão, Visão e aos Valores que refletem a estratégia corporativa da Companhia.

**5.** Devido à informação ser um ativo chave, devem ser tomadas todas as precauções razoáveis para sua proteção.

**6.** A proteção da informação requer que sejam preservadas sua confidencialidade, integridade e disponibilidade. A correta proteção dessas características permitirá à SPA gerar maior valor para os seus clientes, empregados, fornecedores e parceiros.

**7.** Em particular, os processos de negócio executados pela SPA são altamente dependentes de ativos de informação, fazendo com que a segurança da informação e a privacidade, onde aplicável, sejam prioridades para a Companhia.

**8.** Para ser capaz de atender a todos estes requisitos e, ao mesmo tempo, cumprir com os valores corporativos, foi estabelecida uma arquitetura de segurança, onde a Política de Segurança descreve os princípios que devem ser seguidos para a proteção adequada da informação.

**9.** A presente Política de Segurança da Informação e Privacidade contém informações a respeito do modo como a SPA trata, total ou parcialmente, de forma automatizada ou não, os dados pessoais de seus empregados que acessam os sistemas internos e a intranet da SPA. O objetivo é esclarecer acerca dos tipos de dados que são coletados, dos motivos da coleta e da forma como o empregado poderá atualizar, gerenciar ou até excluir algumas destas informações.

**10.** Esta Política estabelece aspectos gerais do Sistema de Gestão da Privacidade da Informação, tais como:

**I.** Definição de Segurança e Privacidade da Informação, e suas importâncias para a SPA;

**II.** Estabelecimento do comprometimento da Alta Gestão com a Segurança e com a Privacidade da Informação;

**III.** Estrutura para Gerenciamento de Riscos de Segurança e de Privacidade da Informação;

**IV.** Explicação geral dos princípios e políticas que norteiam o Sistema de Gestão de Privacidade da Informação (SGPI); e

**V.** Governança (Papéis e Responsabilidades) dentro do SGPI, e estrutura organizacional da SPA.

**11.** São partes integrantes do escopo da presente Política, todos os processos que dão suporte à manutenção da integridade, disponibilidade e confidencialidade das informações necessárias à condução das atividades que fazem parte dos processos de negócio.

## 12. DECLARAÇÃO DE COMPROMISSO DA ALTA GESTÃO

**I.** A Diretoria Executiva da SPA, ciente da importância da informação para o desenvolvimento da sua missão, está comprometida com a preservação da segurança dessa informação e da privacidade.

**II.** Como parte desse compromisso, a SPA praticará os esforços razoáveis e cumprirá com os requerimentos exigidos pela lei para proteger a confidencialidade, integridade e disponibilidade das informações criadas, processadas, armazenadas e transmitidas como parte das suas atividades, bem como à privacidade.

## 13. ESTRUTURA ORGANIZACIONAL

I. A seguir são apresentadas as hierarquias relacionadas com os processos definidos pelo SGPI. Respectivas responsabilidades quanto à Segurança da Informação e Privacidade estão descritas no Capítulo Responsabilidades.


Figura 1 – Estrutura de Decisão

**a) Alta Gestão (DIREXE e CONSAD)**

Grupo composto pela Diretoria Executiva da SPA e pelo Conselho de Administração.

**b) Gestor de Segurança da Informação**

Empregado oficialmente nomeado e responsável pela manutenção do SGPI. Também conhecido como *Security Officer.*

**c) Comitê de Segurança da Informação (CSI)**

O Comitê de Segurança da Informação (CSI) é um grupo multidisciplinar que deve coordenar as atividades de Segurança e Privacidade da Informação em toda a organização.

**d) Gestores**

Empregados oficialmente nomeados e responsáveis pela gestão das unidades organizacionais da SPA.

**e) Empregados**

Todos os empregados, terceiros e prestadores de serviço com funções dentro da estrutura da SPA.

**f) Proprietário da Informação**

Proprietários da Informação são Gerentes, Superintendentes e Diretores das unidades organizacionais que possuem responsabilidade primária por ativos de informação, associados com sua autoridade funcional.

## SEÇÃO II – ABRANGÊNCIA

**14.** A presente Política é aplicável a todos os membros dos órgãos estatutários, empregados da SPA, além dos terceirizados.

## SEÇÃO III – FUNDAMENTAÇÃO LEGAL E NORMATIVA

**15.** A Política de Segurança e Privacidade e SGPI tem como fundamentação legal e normativa:

**I.** Estatuto Social da SPA;

**II.** Resolução CGPAR Nº 11, que determina a necessidade das empresas estatais federais em planejar, implementar e manter práticas de governança de TI, incluindo a formalização e execução de Políticas de Segurança da Informação;

**III.** ISO/IEC 27001:2013, especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta Norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização;

**IV.** ISO/IEC 27002:2013, fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;

**V.** ISO/IEC 27701:2019 Versão Corrigida 2020, especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação (SGPI) na forma de uma extensão das ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para a gestão da privacidade dentro do contexto da organização;

**VI.** COBIT 5 (2012), Modelo Corporativo. para Governança e Gestão de TI da Organização;

**VII.** ACÓRDÃO Nº 1016/2014 – TCU – Plenário, recomenda que a SPA institua práticas de segurança da informação;

**VIII.** Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

**IX.** Decreto nº 9.637/2018, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

**X.** Lei Federal n. 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências;

**XI.** Lei Federal n. 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet); e

**XII.** Lei Federal n. 13.709, de 14/08/2018, que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD).

## SEÇÃO IV – DEFINIÇÕES

**16.** Para os fins desta Política são adotadas as seguintes definições, que poderão ser utilizadas no singular ou plural, sem prejuízo de significado aqui atribuído, e que estão em conformidade com as definições da legislação, com as adaptações necessárias à realidade da SPA:

| Termo | Descrição |
|---|---|
| **Ativos de Informação** | Qualquer informação, sistema, computador, rede de computadores, telecomunicação, mensagem ou serviço de informações pertencentes à SPA. |
| **CSI**<br>**Comitê de Segurança da Informação** | O Comitê de Segurança da Informação (CSI) é um grupo multidisciplinar que deve coordenar as atividades de Segurança da Informação em toda a organização. |
| **SGPI**<br>**Sistema de Gestão da Privacidade da Informação** | Consiste de políticas, procedimentos, guias e outros recursos e atividades associados que são coletivamente gerenciados por uma organização na busca pela proteção de seus ativos de informação, sob a ótica da Segurança da Informação e Privacidade. |
| **SI**<br>**Segurança da Informação** | Envolve a aplicação e o gerenciamento de medidas de segurança apropriadas considerando um leque abrangente de ameaças, com o foco em garantir o sucesso e a continuidade do negócio de forma sustentável, minimizando impactos de incidentes de segurança da informação. Inclui três dimensões principais: confidencialidade, disponibilidade e integridade. |

| Termo | Descrição |
|---|---|
| **TIC**<br>**Tecnologia da Informação e Comunicação** | Conjunto de conhecimentos, sistemas, processos e práticas utilizadas na prestação de serviços de suporte aos processos empresariais de quaisquer naturezas, através de captura, processamento, geração, armazenamento, recuperação e comunicação de dados, informações e conhecimentos. |

## CAPÍTULO II – PRINCÍPIOS

**17.** Os seguintes princípios da presente Política são inegociáveis e impreteríveis à SPA:

**I. Confidencialidade,** diz respeito à divulgação não autorizada de informação sensível para o negócio;

**II. Integridade,** relaciona-se a exatidão, integralidade e autenticidade da informação, bem como a seu valor de acordo com os valores e expectativas da Companhia;

**III. Disponibilidade,** relaciona-se à informação estar disponível quando requerido pelo processo de negócio agora e no futuro;

**IV. Privacidade,** diz respeito à proteção dos dados pessoais, incluindo o respeito, liberdade e as garantias constitucionais do cidadão.

## CAPÍTULO III – DIRETRIZES

### SEÇÃO I – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

**18. OBJETIVOS ESPECÍFICOS**

**I.** Garantir a segurança da informação e privacidade, e padronizar as práticas a serem aplicadas por todo o pessoal com responsabilidade para a segurança da informação e privacidade;

II. Dar consciência dos riscos que ameaçam o sistema de informação e os meios disponíveis para controlá-los;

III. Criar uma estrutura geral para projetar e executar medidas de segurança dos sistemas de informação; e

IV. Promover a cooperação entre os departamentos da SPA para criar, aplicar e verificar as instruções, procedimentos e medidas de segurança relacionadas ao negócio.

## 19. CLASSIFICAÇÃO DA INFORMAÇÃO

I. Considerando a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados, a SPA classifica a informação como a seguir:

| Classificação (Documentos) | Subclassificação (Informação) | Descrição |
|---|---|---|
| **Pública** | Pública | Todos têm acesso (ex: sítio da SPA) |
| **Reservado** | Interna | Todos os funcionários da SPA têm acesso. (ex: lista de aniversariantes) |
| **Sigiloso** | Confidencial | Somente os funcionários de uma organização da SPA tem acesso (ex: Jurídico) |
| | Secreta | Somente uma pessoa, ou a quem esta pessoa designar tem acesso (ex: informações do Presidente da SPA) |

### 19.1. CRITÉRIOS DE CLASSIFICAÇÃO

I. Todas as informações da SPA, assim que criadas, devem ser classificadas de acordo com a sensibilidade da sua Confidencialidade;

II. Cada informação deve ser classificada por seu gestor, denominado Gestor da Informação;

**III.** A sensibilidade da informação de que trata o quadro acima, deve considerar quatro níveis:

**a)** pública;

**b)** interna;

**c)** confidencial; e

**d)** secreta.

**IV.** A informação pública deve ser de conhecimento geral;

**V.** A informação interna somente deve ser conhecida por funcionários da SPA e, em casos específicos, por fornecedores ou terceiros com relação de negócios com a Companhia;

**VI.** A divulgação da informação interna pode gerar efeitos negativos mínimos, criando possíveis incidentes de segurança principalmente pela utilização de técnicas de Engenharia Social;

**VII.** A informação confidencial deve ser de uso exclusivo da organização e de pessoas específicas, por eles designadas; inclui-se nessa classificação os dados pessoais;

**VIII.** A divulgação da informação confidencial poderá criar efeitos negativos de moderados a fortes, afetando notavelmente aspectos financeiros, produtivos, legais e/ou de imagem;

**IX.** É um incidente de segurança da informação o acesso indevido das informações;

**X.** A informação secreta é de conhecimento apenas do Gestor da Informação e por aquelas pessoas especificas, por ele designadas;

**XI.** A divulgação não autorizada da informação secreta poderá criar efeitos fortes e permanentemente desastrosos, afetando aspectos financeiros, produtivos, legais e/ou de imagem;

**XII.** O Gestor da Informação, deve revisar ao menos anualmente:

**a)** a classificação, por ele definidas, das suas informações; e

**b)** os privilégios de acesso à informação classificada.

**XIII.** A revisão tem como objetivo identificar e atualizar controles de acesso que não correspondam com os requisitos de funcionalidade e/ou segurança do negócio;

**XIV.** A classificação da informação, deve considerar:

**a)** os requisitos de Informação segundo o aspecto de:

- Confidencialidade;
- Integridade; e
- Disponibilidade.

**b)** as normas e regras legais aplicáveis.

**XV.** A classificação da informação é passível de mudanças durante o seu ciclo de vida de acordo com a necessidade de variação em sua sensibilidade; e

**XVI.** Informações agrupadas (ex.: documento juntado, armazenamento em disco rígido etc.) devem ser classificadas de acordo com o nível de classificação mais sensível do grupo;

**XVII.** Toda informação classificada como confidencial deve ser mantida criptografada durante todo o ciclo de vida da informação, desde a criação até seu descarte/eliminação;

**XVIII.** Os registros de log das aplicações são considerados, por padrão, como confidenciais. Com o apoio da Gerência de Infraestrutura de Dados na

identificação dos dados armazenados, a sua classificação é passível de mudança caso o gestor do sistema entenda a necessidade.

**XIX.** Para cada informação classificada, o Gestor da Informação deve definir o requisito de privilégio mínimo para seu acesso (princípio *Least Privilege*), identificando:

**a)** as pessoas autorizadas a acessar a informação;

**b)** os privilégios adequados com as necessidades do processo (princípio *Need-to-know*) para uso da informação:

- leitura;
- criação;
- modificação;
- exposição;
- cópia em dispositivos pessoais ou impressão;
- compartilhamento via e-mail; e
- eliminação.

**XX.** Todos os requisitos acima devem ser listados e distribuídos física ou eletronicamente e somente podem ser manipulados por pessoas autorizadas.

## 20. REQUISITOS GERAIS DE MANIPULAÇÃO DAS INFORMAÇÕES

**I.** São requisitos gerais de manipulação de uma informação:

**a) Distribuição:**

- versões eletrônicas do documento devem ser disponibilizadas em formato não alterável após a liberação (PDF/A).

**b) Armazenamento e Transporte:**

- as mídias extraíveis que contenham informações com diferentes classificações devem ser protegidas de acordo com a classificação da informação mais sensível; e
- antes do transporte de informações em mídias extraíveis, deve haver verificação da existência de outras informações mais sensíveis no dispositivo que não serão transportadas.

**c) Rotulagem:**

- o rótulo dos meios de informação (mídias de backup, e-mail, documento físico etc.) devem identificar a classificação da informação mais sensível.

**d) Descarte:**

- o descarte das informações em formato digital deve considerar as diretrizes definidas no INP-SUPTI-TIC-140-012-Segurança nas Operações.

## 21. CONSIDERAÇÕES GERAIS

**I.** É responsabilidade da organização onde o funcionário está lotado, a proteção de seus dados pessoais e corporativos utilizados na execução de suas atividades e tarefas;

**II.** Os sistemas de informação com acesso público devem ser verificados periodicamente pelos Gestores da informação disponibilizada contra eventuais falhas de integridade. A periodicidade deve ser:

**a)** no mínimo, de uma vez ao ano; ou

**b)** conforme necessidade.

**III.** A Gerência de Infraestrutura de Dados deve definir, com o apoio dos Gestores das informações, os controles tecnológicos para identificar fragilidades antes de a informação ser disponibilizada, de acordo com as

diretrizes de manipulação das informações apresentadas resumidamente no ANEXO 1;

**IV.** As diretrizes sobre a gestão documental, estão descritas nos normativos internos da SPA que tratam de gestão documental.

**SEÇÃO II – TRATAMENTO E PROTEÇÃO DOS DADOS PESSOAIS**

## 22. CONSIDERAÇÕES

### 22.1. DIREITOS DO EMPREGADO

**I.** A SPA, por meio da intranet e dos sistemas internos, se compromete a cumprir as normas previstas na LGPD – Lei Geral de Proteção de Dados, em respeito aos seguintes princípios:

**a)** Os dados pessoais do empregado serão tratados de forma lícita, leal e transparente **(licitude, lealdade e transparência)**;

**b)** Os dados pessoais do empregado serão coletados apenas para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades **(limitação das finalidades)**;

**c)** Os dados pessoais do empregado serão coletados de forma adequada, pertinente e limitada às necessidades do objetivo para os quais eles são processados **(minimização dos dados)**;

**d)** Os dados pessoais do empregado serão mantidos exatos, e atualizados sempre que necessário, de maneira que os dados inexatos sejam retificados quando possível e apagados se necessário **(exatidão)**;

**e)** Os dados pessoais do empregado serão conservados de uma forma que permita a identificação dos Titulares dos dados (empregado) apenas durante o período necessário para as finalidades para as quais são tratados **(limitação da conservação)**; e

**f)** Os dados pessoais do empregado serão tratados de forma segura, protegidos do tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizacionais adequadas **(integridade e confidencialidade)**.

**II.** O empregado que navega pela intranet ou sistemas internos da SPA possui os seguintes direitos, conferidos pela Lei de Proteção de Dados Pessoais:

**a)** **Direito de confirmação e acesso:** é direito do empregado, da SPA, a confirmação de que os dados pessoais que lhe digam respeito, são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais;

**b)** **Direito de retificação:** é direito do empregado de obter, sem demora injustificada, a retificação dos dados pessoais inexatos que lhe digam respeito, constantes da intranet e dos sistemas internos da SPA;

**c)** **Direito à eliminação dos dados (direito ao esquecimento):** é direito do empregado de ter seus dados apagados da intranet ou dos sistemas internos da SPA, ao término da finalidade específica do motivo da retenção;

**d)** **Direito à limitação do tratamento dos dados:** é direito do empregado, de limitar o tratamento de seus dados pessoais, podendo exercê-lo quando contestar a exatidão dos dados, quando o tratamento for ilícito, quando a SPA não precisar mais dos dados para as finalidades propostas, quando tiver manifestado oposição ao tratamento dos dados e em caso de tratamento de dados desnecessários;

**e)** **Direito de oposição:** é direito do empregado de, a qualquer momento, se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito; e

**f)** **Direito de não ser submetido a decisões automatizadas:** é direito do empregado de não ficar sujeito a nenhuma decisão tomada

exclusivamente com base no tratamento automatizado, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

**III.** O empregado poderá exercer os seus direitos através do formulário e instruções contidos na URL http://www.portodesantos.com.br/informacao/termo-de-privacidade/

**IV.** O empregado será informado em caso de retificação ou eliminação dos seus dados.

### 22.2. DEVER DE NÃO FORNECER DADOS DE TERCEIROS

**I.** Durante a navegação pela intranet ou sistemas internos da SPA, a fim de resguardar e de proteger os direitos de terceiros, o empregado da SPA deverá fornecer – quando solicitado – somente seus dados pessoais, e não os de terceiros.

### 22.3. INFORMAÇÕES COLETADAS

**I.** A coleta de dados dos empregados se dará em conformidade com o disposto nesta Política de Segurança da Informação e Privacidade e dependerá do consentimento do empregado, sendo este dispensável somente nas hipóteses previstas no art. 11, inciso II, da Lei de Proteção de Dados Pessoais.

### 22.4. TIPOS DE DADOS COLETADOS

**I. Dados de identificação do empregado para realização de cadastros**

A utilização, pelo empregado, de determinadas funcionalidades da intranet ou dos sistemas internos da SPA dependerá de cadastro, sendo que, nestes casos, vários dados do empregado poderão ser coletados e armazenados:

a) **Dados informados em algum formulário de contato**

Os dados eventualmente informados pelo empregado que utilizar algum formulário de contato disponibilizado na intranet ou sistemas internos da SPA, incluindo o teor da mensagem enviada, serão coletados e armazenados.

b) **Registros de acesso**

Em atendimento às disposições do art. 15, caput e parágrafos, da Lei Federal n. 12.965/2014 (Marco Civil da Internet), os registros de acesso do empregado serão coletados e armazenados pelo tempo legal para retenção dos mesmos.

c) **Newsletter**

No caso de a SPA publicar uma newsletter, o endereço de e-mail cadastrado pelo empregado que optar por se inscrever nesta Newsletter será coletado e armazenado até que o empregado solicite seu descadastro.

d) **Dados sensíveis**

Será coletado pela intranet ou pelos sistemas internos da SPA, quando necessário, dados sensíveis dos empregados, cuja forma de tratamento está definida nos termos dos arts. 9º a 11 e demais dispositivos da Lei de Proteção de Dados Pessoais – LGPD. Assim, dentre outros, haverá coleta dos seguintes dados:

- Dados que revelem sua origem racial ou étnica, e/ou a filiação sindical do empregado;
- Dados genéticos;
- Dados biométricos para identificar uma pessoa de forma inequívoca;
- Dados relativos à saúde do empregado; e
- Dados relacionados a condenações penais ou a infrações ou com medidas de segurança conexas.

**e) Coleta de dados não previstos expressamente**

Eventualmente, outros tipos de dados não previstos expressamente nesta Política de Segurança da Informação e Privacidade poderão ser coletados, desde que seja indicada a finalidade e sejam fornecidos com o consentimento explicito do empregado, ou, ainda, que a coleta seja permitida ou imposta por lei.

## 22.5. FUNDAMENTO JURÍDICO PARA O TRATAMENTO DOS DADOS PESSOAIS

**I.** Ao utilizar os serviços da intranet ou dos sistemas internos da SPA, o empregado está consentindo com a presente Política de Segurança da Informação e Privacidade;

**II.** Nestes casos específicos e enquanto durar o vínculo profissional entre o empregado e a SPA, o empregado não tem o direito de revogar seu consentimento para acessar a intranet ou os sistemas internos da SPA, não comprometendo a licitude do tratamento de seus dados pessoais;

**III.** O tratamento de dados pessoais sem o consentimento do empregado, apenas será realizado em razão de interesse legítimo da SPA ou para as hipóteses previstas em lei, ou seja, dentre outras, as seguintes:

**a)** Para o cumprimento de obrigação legal ou regulatória pelo controlador (SPA);

**b)** Para a realização de estudos por órgão de pesquisa, sendo garantida ao empregado, sempre que possível, a anonimização dos dados pessoais;

**c)** Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o empregado;

**d)** Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

**e)** Para a proteção da vida ou da incolumidade física do titular dos dados ou de terceiros;

**f)** Para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

**g)** Quando necessário para atender aos interesses legítimos da SPA como controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular dos dados que exijam a proteção dos dados pessoais; e

**h)** Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

## 22.6. FINALIDADES DO TRATAMENTO DOS DADOS PESSOAIS

**I.** Os dados pessoais do empregado coletados pela intranet ou pelos sistemas internos da SPA têm por finalidade facilitar, agilizar e cumprir os compromissos estabelecidos entre a SPA e o empregado, bem como fazer cumprir as solicitações realizadas por meio do preenchimento de formulários diversos;

**II.** Os dados pessoais poderão ser utilizados também para a finalidade de personalizar o conteúdo oferecido ao empregado, bem como para dar subsídio à intranet ou algum sistema interno da SPA visando a otimizar a qualidade e funcionamento de seus serviços;

**III.** Os dados de qualquer cadastro serão utilizados para permitir o acesso do empregado a determinados conteúdos da intranet ou de sistemas internos da SPA, exclusivos para os empregados devidamente cadastrados; e

**IV.** O tratamento de dados pessoais para finalidades não previstas nesta Política de Segurança da Informação e Privacidade somente ocorrerá mediante comunicação prévia ao empregado, sendo que, em qualquer caso, os direitos e obrigações aqui previstos permanecerão aplicáveis.

## 22.7. PRAZO DE CONSERVAÇÃO DOS DADOS PESSOAIS

**I.** Os dados pessoais do empregado serão conservados por um período não superior ao definido por uma "tabela de temporalidade" específica ou, na ausência desta, a legislação pertinente ao assunto, para cumprir os objetivos legais e regulatórios em razão dos quais eles são processados.

**II.** O período de conservação dos dados é definido de acordo com os seguintes critérios:

**a)** Os dados serão armazenados pelo tempo necessário para a prestação dos serviços fornecidos pela intranet ou pelos sistemas internos da SPA ao empregado, de acordo com a legislação ou regulação aplicáveis ou pode variar de 1 a 6 meses, em caso de não existir legislação regulatória aplicável;

**b)** Os dados pessoais dos empregados apenas poderão ser conservados após o término de seu tratamento nas seguintes hipóteses:

**1.** Para o cumprimento de obrigação legal ou regulatória pelo controlador (SPA);

**2.** Para estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

**3.** Para a transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na legislação; e

4. Para uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que os dados sejam anonimizados.

## 22.8. DESTINATÁRIOS E TRANSFERÊNCIA DOS DADOS PESSOAIS

I. Os dados pessoais dos empregados poderão ser compartilhados com terceiros (que serão identificados como operadores e/ou controladores no âmbito da Lei 13.709/2018) para cumprimento de obrigações legais por parte da SPA em favor dos empregados. Os dados serão, portanto, tratados não só pela SPA como por esses terceiros por instrução da SPA.

## 22.9. DO TRATAMENTO DOS DADOS PESSOAIS

### 22.9.1. DO RESPONSÁVEL PELO TRATAMENTO DOS DADOS (DATA CONTROLLER)

I. A SPA, na condição de controlador, é responsável pelo tratamento dos dados pessoais do empregado, bem como, por determinar as finalidades e os meios de tratamento de dados pessoais.

II. Na intranet da SPA e nos sistemas internos da SPA, o responsável pelo tratamento dos dados pessoais coletados é o Encarregado pelo Tratamento de Dados Pessoais da Autoridade Portuária de Santos, que poderá ser contactado pelo e-mail: etdp@brssz.com ou através do formulário da URL. http://www.portodesantos.com.br/informacao/termo-de-privacidade/

III. O responsável pelo tratamento dos dados se encarregará diretamente do tratamento dos dados pessoais dos empregados.

### 22.9.2. SEGURANÇA NO TRATAMENTO DOS DADOS PESSOAIS DO EMPREGADO

**I.** A SPA se compromete a aplicar as medidas técnicas e organizativas aptas a proteger os dados pessoais de seus empregados contra acessos não autorizados bem como de situações de destruição, perda, alteração, comunicação ou difusão indevida de tais dados;

**II.** Para a garantia da segurança, serão adotadas soluções que levem em consideração: as técnicas adequadas; os custos de aplicação; a natureza, o âmbito, o contexto e as finalidades do tratamento; e os riscos para os direitos e liberdades do empregado;

**III.** A intranet da SPA utiliza certificado SSL (*Secure Socket Layer*) que garante que os dados pessoais sejam trafegados de maneira segura e confidencial, a fim de que a transmissão dos dados entre o servidor e o empregado, e a retroalimentação, ocorram de forma totalmente cifrada ou criptografada;

**IV.** No entanto, a SPA se exime de responsabilidade por eventuais falhas de segurança da intranet e dos sistemas internos da SPA que vierem a ocorrer por culpa exclusiva de terceiros, como em caso de ataque de hackers ou crackers, ou culpa exclusiva do empregado, como no caso em que ele mesmo transfira ou forneça seus dados a um terceiro. A intranet e os sistemas internos da SPA conterão mecanismos para comunicar o empregado, em prazo adequado, caso ocorra algum tipo de violação da segurança de seus dados pessoais que possa lhe causar um “alto risco” para seus direitos e liberdades pessoais;

**V.** A violação de dados pessoais é uma violação de segurança que provoca, de modo acidental ou intencional, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizado a dados pessoais que foram transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento; e

**VI.** Por fim, a SPA assume compromisso de que os dados pessoais do empregado, obtidos por meio da intranet e dos sistemas internos da SPA serão tratados com confidencialidade, dentro dos limites legais.

### 22.9.3. DADOS DE NAVEGAÇÃO (COOKIES)

**I.** *Cookies* são pequenos arquivos de texto enviados pela intranet da SPA ao computador do empregado e que nele ficam armazenados, com informações relacionadas à navegação do site da intranet da SPA;

**II.** Por meio dos *cookies*, pequenas quantidades de informação são armazenadas pelo navegador do empregado para que o servidor da SPA possa acessá-las e tratá-las posteriormente. Podem ser armazenados, por exemplo, dados sobre o dispositivo utilizado pelo empregado, bem como seu local e horário de acesso ao site da intranet da SPA;

**III.** Os *cookies* não permitem e não foram projetados para que qualquer arquivo ou informação sejam acessados ou extraídos do disco rígido do empregado, não sendo possível, ainda, que, por meio deles, se tenha acesso a informações pessoais que não tenham partido dele ou da forma como utiliza os recursos do site da intranet da SPA;

**IV.** É importante ressaltar que nem todo *cookie* contém informações que permitem a identificação do empregado, sendo que determinados tipos podem ser utilizados simplesmente para que o site da intranet da SPA seja carregado corretamente, ou para que suas funcionalidades atuem do modo esperado; e

**V.** As informações eventualmente armazenadas em *cookies* que permitam identificar um empregado são consideradas dados pessoais. Dessa forma, todas as regras previstas nesta Política de Segurança da Informação e Privacidade também lhes são aplicáveis.

### 22.9.4. COOKIES DA INTRANET DA SPA

**I.** Os *cookies* utilizados na intranet da SPA são aqueles enviados ao computador ou dispositivo do empregado exclusivamente pelo servidor da SPA;

**II.** As informações coletadas por meio destes *cookies* são utilizadas para melhorar e personalizar a experiência de acesso e navegação do empregado, sendo que alguns podem, por exemplo, ser utilizados para lembrar as preferências e escolhas do empregado; e

**III.** Estes dados de navegação não serão compartilhados com eventuais terceiros, buscando, por exemplo, o aprimoramento de produtos e/ou serviços ofertados ao empregado.

### 22.9.5. GESTÃO DOS COOKIES E CONFIGURAÇÕES DO NAVEGADOR

**I.** O empregado poderá se opor ao registro de cookies pela intranet da SPA, bastando que desative esta opção no seu próprio navegador ou dispositivo móvel;

**II.** A desativação dos *cookies*, no entanto, pode afetar a disponibilidade de algumas ferramentas e funcionalidades da intranet da SPA, comprometendo seu correto e esperado funcionamento. Outra consequência possível é a remoção das preferências do empregado que eventualmente tiverem sido salvas, prejudicando sua experiência de navegação; e

**III.** A seguir, são disponibilizados alguns links para as páginas de ajuda e suporte dos navegadores mais utilizados, que poderão ser acessadas pelo empregado interessado em obter mais informações sobre a gestão de cookies em seu navegador:

**a)** Internet Explorer: https://support.microsoft.com/pt-br/help/17442/windows-internet-explorer-delete-manage-cookies

**b)** Safari: https://support.apple.com/pt-br/guide/safari/sfri11471/mac

**c)** Google Chrome: https://support.google.com/chrome/answer/95647?hl=pt-BR&hlrm=pt

**d)** Mozila Firefox: https://support.mozilla.org/pt-BR/kb/ative-e-desative-os-cookies-que-os-sites-usam

**e)** Opera: https://www.opera.com/help/tutorials/security/privacy/

### 22.10. RECLAMAÇÃO A UMA AUTORIDADE DE CONTROLE

**I.** Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação à Agência Nacional de Proteção de Dados (Autoridade de Controle). A reclamação poderá ser feita ao Encarregado pelo tratamento de Dados pessoais da SPA, do país de residência habitual do empregado, do seu local de trabalho ou do local onde foi alegadamente praticada a infração.

## 23. DAS ALTERAÇÕES

**I.** Esta Política de Segurança da Informação e Privacidade poderá ser revisada a qualquer momento em decorrência de eventual atualização na estratégia corporativa da SPA, razão pela qual se recomenda consultar periodicamente este documento;

**II.** A SPA se reserva o direito de modificar, a qualquer momento as presentes disposições, especialmente para adaptá-las às evoluções do site http://intranet.portodesantos.com.br/ e seus sistemas, seja pela

disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes; e

**III.** O empregado poderá ser (caso solicite) explicitamente notificado em caso de alteração desta Política.

## 24. DO DIREITO APLICÁVEL E DO FORO

**I.** Para a solução das controvérsias decorrentes do presente instrumento, será aplicado integralmente o Direito brasileiro; e

**II.** Os eventuais litígios deverão ser apresentados no Foro de Santos.

## 25. CONTROLES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

**I.** Os controles de segurança consistem em um conjunto amplo de medidas de segurança, visando a minimizar os riscos presentes nos ativos de Informação. Os controles são baseados na norma de segurança aceita internacionalmente (ISO 27001/27002 e a extensão 27701), nas especificações de segurança impostas pelos Instrumentos Normativos de Processo e aprovados pela Diretoria Executiva.

## 26. IMPLANTAÇÃO E AVALIAÇÃO

**I.** A SPA deve estar em conformidade com os requisitos desta Política. Os requisitos podem ser revisados para atender as necessidades de parceiros e da própria Companhia. O processo de verificação da conformidade desta deve ser conduzido pela Superintendência de Governança, Riscos e *Compliance* (SUGOV) obedecendo às políticas, normas e procedimentos definidos no SGPI.

## 27. EXCEÇÃO À POLÍTICA

**I.** As exceções serão avaliadas e devem ser reportadas por escrito ao Comitê de Segurança da Informação. Este irá avaliar as exceções conforme as

justificativas de negócio fornecidas pelo solicitante e definir o tratamento adequado.

## SEÇÃO III – SGPI – SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO

### 28. RISCO

**I.** O Sistema de Gestão de Privacidade da Informação da SPA está voltado para a mitigação do risco dos ativos de informação e da privacidade;

**II.** A SPA entende que o gerenciamento dos riscos em segurança da informação e de privacidade é um processo cíclico e dinâmico que requer uma constante participação de todas as pessoas. Devido ao fato de ser um processo cíclico, está em constante evolução e aprimoramento mediante a comparação dos resultados do processo com os resultados esperados e ajuste das entradas para melhorá-los;

**III.** O processo de gerenciamento do risco está baseado nas seguintes etapas:

- **a)** Identificação dos ativos críticos;
- **b)** Levantamento e avaliação dos riscos associados a esses ativos;
- **c)** Criação de um plano para o tratamento desses riscos; e
- **d)** Execução do plano de tratamento de riscos.

**IV.** O processo é cíclico no sentido de que após a execução do plano de tratamento de riscos, o novo nível de risco deve ser comparado (chamado de risco residual) com o nível avaliado inicialmente;

**V.** A informação resultante dessa comparação deve ser utilizada para iniciar novamente o processo; e

**VI.** O processo é dinâmico também no sentido de que os ativos críticos de informação mudam ao longo do tempo e, portanto, devem ser avaliados periodicamente para manter a sua identificação atualizada com os processos de negócio.

## 29. REQUISITOS

### 29.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (ESTE DOCUMENTO)

**I.** O Objetivo deste documento é capacitar a Diretoria Executiva no sentido de assegurar a execução e manutenção das orientações e estratégias do SGPI definidas pelo Conselho de Administração de acordo com os objetivos de negócio, bem como com as leis e regulamentações relevantes.

### 29.2. ORGANIZAÇÃO DA SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

**I.** Uma Estrutura Organizacional de gerenciamento deve ser estabelecida para iniciar e controlar a operação da Segurança e Privacidade da Informação na SPA; e

**II.** Esta Estrutura Organizacional deve ser responsável por estabelecer os procedimentos de utilização de dispositivos móveis e trabalho remoto.

### 29.3. RECURSOS HUMANOS

**I.** Devem existir procedimentos específicos em Segurança e Privacidade da Informação para os processos de contratação do empregado, durante o seu contrato de trabalho, bem como as mudanças e o encerramento do contrato.

### 29.4. GESTÃO DE ATIVOS DE INFORMAÇÃO

**I.** Deve ser implementado um procedimento de responsabilidade pela proteção dos ativos de informação;

**II.** Todas as informações devem ser devidamente classificadas quanto ao nível adequado de proteção, de acordo com a sua importância para o negócio; e

**III.** Deve existir um procedimento que evite a divulgação, alteração ou cópia não autorizada de qualquer informação armazenada em qualquer tipo de mídia de propriedade da SPA.

### 29.5. CONTROLE DE ACESSO

**I.** Deve existir um conjunto de procedimentos que controle o acesso à informação, aos ativos e recursos de processamento da informação e que garanta ao usuário acesso autorizado a sistemas e serviços existentes para o exercício de suas funções ao mesmo tempo que previna o acesso não autorizado aos mesmos sistemas e serviços; e

**II.** Todos os usuários devem ser responsáveis pela proteção das informações necessárias para a sua autenticação em sistemas e serviços da SPA.

### 29.6. USO DE CRIPTOGRAFIA

**I.** Procedimentos de criptografia devem ser utilizados de forma efetiva e adequada para proteger a confidencialidade, autenticidade e/ou a integridade da informação.

### 29.7. SEGURANÇA FÍSICA DO AMBIENTE DE TRABALHO

**I.** Devem existir procedimentos que previnam o acesso físico não autorizado, incluindo danos, furtos e comprometimento de ativos, e interferências aos sistemas, recursos e serviços de processamento das informações que suportam a SPA.

### 29.8. SEGURANÇA DAS OPERAÇÕES

**I.** Devem existir procedimentos que garantam a operação segura e correta dos sistemas, recursos e serviços de processamento da informação, incluindo proteção contra *malware*, controle de cópias de segurança, Sistemas Operacionais, registros e monitoramento das operações, além

de um Sistema de Gestão de Vulnerabilidades Técnicas, visando a prevenção e controle do risco associado com a exploração indevida por parte de hackers, das possíveis vulnerabilidades técnicas encontradas em sistemas operacionais, sistemas e serviços disponíveis para os empregados.

**II.** Todos os sistemas de informação devem ser periodicamente auditados visando a minimizar o impacto do mau uso ou do uso ineficiente de tais sistemas.

### 29.9. SEGURANÇA DAS COMUNICAÇÕES

**I.** A segurança das redes deve ser assegurada visando a proteção das informações e recursos de processamento das informações que as apoiam; e

**II.** Toda a informação transferida internamente ou de/para terceiros deve ser devidamente protegida em função de sua classificação quanto à confidencialidade.

### 29.10. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

**I.** Devem existir garantias de que a segurança da informação seja parte integrante de todo ciclo de vida dos sistemas de informação, incluindo os requisitos para o desenvolvimento de sistemas e a devida proteção e privacidade dos dados utilizados para teste.

### 29.11. RELACIONAMENTO COM FORNCEDORES E TERCEIROS

**I.** Devem existir procedimentos que garantam a proteção dos ativos de informação, sistemas, recursos e serviços da SPA que são acessados por terceiros.

### 29.12. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

**I.** Devem existir procedimentos para gerenciar os incidentes de segurança da informação, incluindo a comunicação de vulnerabilidades encontradas e ocorrência de eventos.

### 29.13. GESTÃO DA CONTINUIDADE DO NEGÓCIO

**I.** Devem existir procedimentos que garantam a continuidade do negócio em face de incidentes de segurança da informação.

### 29.14. CONFORMIDADE (COMPLIANCE)

**I.** Devem existir procedimentos que garantam a conformidade com obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação ou quaisquer requisitos de segurança da informação, e para assegurar que o SGPI esteja implementado e operado de acordo com as políticas, procedimentos da SPA.

## CAPÍTULO IV – RESPONSABILIDADES

**30.** No âmbito da presente Política, as instâncias e unidades de gestão abaixo elencadas são responsáveis, além das suas respectivas atribuições previstas no Estatuto Social, Regimento Interno próprio ou Regimento Interno da Companhia, por:

**I.** **COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI),** grupo multidisciplinar que deve coordenar as atividades de Segurança da Informação em toda a SPA.

**II.** **CONSELHO DE ADMINISTRAÇÃO (CONSAD),** responsável por:

**a)** Aprovar a presente Política;

**b)** Definir e desenvolver as estratégias de Segurança da Informação e Privacidade em alinhamento com o Plano Estratégico da SPA; e

**c)** Acompanhar as ações da Diretoria Executiva relacionadas à Segurança da Informação e Privacidade.

**III. DIRETORIA EXECUTIVA (DIREXE),** responsável por:

**a)** Garantir o atendimento das Políticas de Segurança da Informação e o funcionamento do SGPI;

**b)** Garantir a compatibilidade da segurança da informação com os objetivos estratégicos da Companhia;

**c)** Aprovar as iniciativas para a melhoria contínua do SGPI;

**d)** Prover recursos para a gestão, operação e monitoramento adequado das atividades do SGPI;

**e)** Suportar perante toda a Companhia as iniciativas da Área de Segurança da Informação;

**f)** Garantir a contínua manutenção das Políticas de Segurança da Informação e desdobramento de seus respectivos objetivos;

**g)** Garantir a contínua análise e realimentação dos resultados de gestão de riscos ao SGPI;

**h)** Comprometer-se nas aprovações:

- dos documentos oriundos do SGPI; e
- das aquisições de recursos para a melhoria do SGPI.

**i)** Ter conhecimento das auditorias conduzidas nos sistemas para que os planos de ação sejam cumpridos.

**IV. GESTOR DE SEGURANÇA DA INFORMAÇÃO,** responsável por:

**a)** Produzir diretivas locais de segurança, regras e padrões a serem usados pelos empregados;

**b)** Propor os recursos necessários às ações de segurança da informação e comunicações;

**c)** Coordenar o Comitê de Segurança da Informação e Comunicações - CSI;

**d)** Desenvolver e promover programas de conscientização de segurança;

**e)** Garantir que todos os gestores estejam cientes de suas próprias responsabilidades relacionadas à Segurança da Informação;

**f)** Certificar-se que o processo de Gestão de Pessoas leva em conta todos os aspectos de Segurança da Informação ao contratar novos empregados, ou durante o vínculo empregatício, ou em rescisão de contratos de trabalho;

**g)** Revisar periodicamente o nível de segurança de sistemas internos, emitindo avisos após estas revisões. Analisar criticamente, em intervalos periódicos, o progresso dos planos de melhoria resultantes em conjunto com os gestores envolvidos;

**h)** Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;

**i)** Analisar criticamente os incidentes de segurança mais significativos e gerenciar e/ou acompanhar as ações relacionadas na solução dos mesmos;

**j)** Representar a SPA, interna e externamente, nos assuntos relacionados ao SGPI;

**k)** Gerenciar os processos do SGPI, na busca da melhoria contínua e alinhamento com a Alta Gestão;

**l)** Realizar a coleta de dados e informações pertinentes à segurança da informação para a realização de análise crítica pela Diretoria;

**m)** Dar retorno dos resultados das análises críticas feitas pela Direção, aos envolvidos visando possíveis providências;

**n)** Acompanhar o sistema de ações corretivas e preventivas do SGPI; e

**o)** Garantir a contínua manutenção e atualização dos indicadores de desempenho dos processos do SGPI, estimulando melhorias e mudanças de metas.

V. **GESTORES,** responsáveis por:

**a)** Manter atualizada a definição dos ativos de informação e notificar em qualquer alteração no inventário de ativos de sua área;

**b)** Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto a proteção da Segurança da Informação em sua área de atuação;

**c)** Informar/comunicar todos os fatos relacionados ao SGPI às áreas de operação sob sua responsabilidade;

**d)** Contribuir para implantação dos objetivos de gestão de Segurança da Informação e efetuar as medições necessárias por processos;

**e)** Implantar as oportunidades de melhoria;

**f)** Planejar a adoção de procedimentos do SGPI e monitorar sua eficácia em sua área de atuação; e

**g)** Garantir a contínua eficácia dos controles implantados para satisfazer os requisitos do SGPI.

VI. **EMPREGADOS E TERCEIRIZADOS DA SPA,** responsáveis por:

**a)** Notificar seus gestores sobre qualquer alteração no inventário de ativos de sua área;

**b)** Conhecer e seguir os procedimentos constantes no SGPI;

**c)** Recomendar melhorias no SGPI;

**d)** Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro da SPA; e

**e)** Cuidar pela proteção dos ativos de informação a que tiverem acesso.

VII. **PROPRIETÁRIOS DA INFORMAÇÃO (Gerentes, Superintendentes e Diretores da SPA),** responsáveis por:

**a)** Definir e atualizar os ativos de informação;

**b)** Determinar os requerimentos de confidencialidade, integridade e disponibilidade para proteger esses ativos de informação relacionados com os processos de negócio ao seu cargo;

**c)** Definir procedimentos que estejam alinhados aos princípios e diretrizes de Segurança da Informação;

**d)** Segregar funções e separar recursos de desenvolvimento, teste e produção dentro dos seus processos de negócio;

**e)** Os proprietários da informação gerenciarão a correta prestação de serviços por parte de terceiros que afetem/suportem a segurança dos ativos de informação ao seu cargo, fazendo análise crítica do seu desempenho e possíveis oportunidades de melhoria; e

**f)** É responsabilidade do proprietário da informação a realização de análise crítica em seus processos de negócio e em particular dos riscos à informação.

## CAPÍTULO V – SANÇÕES

**31.** A não observância desta Política e de seus desdobramentos normativos implicará, no que couber, em sanções previstas no Regulamento Interno de Pessoal (RIP) e/ou no Código de Ética da SPA.

## CAPÍTULO VI – DISPOSIÇÕES GERAIS

**32.** Compete aos gestores da Companhia difundir a presente Política e seus desdobramentos aos empregados e zelar por seu cumprimento; e

**33.** É dever dos administradores e empregados da Companhia observar os princípios e procedimentos estabelecidos neste documento.

## ANEXO 1 – TERMO DE RESPONSABILIDADE INDIVIDUAL

Santos/SP, _____ de _____ de _____

Pelo presente instrumento, eu, _____ _____ (nome/registro), perante a Santos Port Authority, doravante denominada SPA, na qualidade de usuário do ambiente computacional de propriedade da referida Companhia, declaro estar ciente das normas de segurança das informações digitais da SPA, segundo as quais devo:

a) tratar a informação digital como patrimônio da SPA e como um recurso que deva ter seu sigilo preservado, em consonância com a legislação vigente;

b) utilizar as informações disponíveis e os sistemas e produtos computacionais, dos quais a SPA é proprietária ou possui o direito de uso, exclusivamente para o interesse do serviço;

c) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas;

d) não tentar obter acesso à informação cujo grau de sigilo não seja compatível com o que possuo na Companhia ou que eu não tenha autorização ou necessidade de conhecer;

e) não compartilhar o uso de senha com outros usuários;

f) não me passar por outro usuário usando ardilosamente sua identificação de acesso e senha;

g) não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de meu uso;

h) instalar e utilizar em meu microcomputador somente programas homologados para uso na SPA e que esta possua as respectivas licenças de uso ou, no caso de programas de domínio público, mediante autorização formal da área de informática da SPA;

i) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o conteúdo das informações

e documentos sigilosos a que tive acesso e não os divulgar a pessoas não autorizadas;

j) guardar segredo das minhas autenticações de acesso (senhas) utilizadas no ambiente computacional da SPA, não cedendo, não transferindo, não divulgando e não permitindo o seu conhecimento por terceiros;

k) não utilizar senha com sequência fácil ou óbvia de caracteres que facilite a sua descoberta e não escrever a senha em lugares visíveis ou de fácil acesso;

l) ao me afastar momentaneamente da minha estação de trabalho, utilizar descanso de tela (screen saver) protegido por senha, a fim de evitar que alguém possa ver as informações que estejam disponíveis na tela do computador;

m) ao me ausentar do local de trabalho, momentaneamente ou ao término de minhas atividades diárias, certificar-me de que a sessão aberta no ambiente computacional com minha identificação foi fechada e as informações que exigem sigilo foram adequadamente salvaguardadas;

n) seguir as orientações da área de informática da SPA relativas à instalação, à manutenção e ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;

o) comunicar imediatamente ao meu superior hierárquico e à área de informática da SPA a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de segurança estabelecidos;

p) responder, perante a SPA, as auditorias e a área de informática da SPA, por acessos, tentativas de acessos ou uso indevido da informação digital realizados com a minha identificação ou autenticação;

q) não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;

r) estar ciente de que toda informação digital armazenada e processada no ambiente computacional da SPA pode ser auditada, como no caso de páginas informativas (sites) visitadas por mim;

s) não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;

t) não transferir qualquer tipo de arquivo que pertença à SPA para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;

u) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da SPA;

v) estar ciente de que a SPA poderá auditar os arquivos em trâmite ou armazenados nos equipamentos do ambiente computacional da SPA sob meu uso ou responsabilidade;

w) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da SPA deve obedecer a este preceito; e

x) estar ciente de que a SPA poderá auditar as correspondências eletrônicas originadas ou retransmitidas por mim no ambiente computacional da SPA.

Desta forma, estou ciente da minha responsabilidade pelas consequências decorrentes da não observância do acima exposto e da legislação vigente.

_____

Assinatura
Nome Completo/registro

# INFORMAÇÕES DE CONTROLE

**TÍTULO**

**POLÍTICA DE SEGURANÇA E PRIVACIDADE E SGPI**

**VERSÃO**

0.0.1 (é a primeira versão em forma de Política)

**UNIDADE GESTORA DO DOCUMENTO**

SUPERVISÃO DE GOVERNANÇA DE TI

**ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR**

PRIMEIRA VERSÃO

**RELAÇÃO COM OUTROS NORMATIVOS INTERNOS**

ESTATUTO SOCIAL

INP-SUPTI-TIC-140-007-Recursos Humanos
INP-SUPTI-TIC-140-008-Gestão de Ativos
INP-SUPTI-TIC-140-009-Gestao de Acesso
INP-SUPTI-TIC-140-010-Criptografia
INP-SUPTI-TIC-140-011-Segurança física e ambiente
INP-SUPTI-TIC-140-012-Segurança nas Operações
INP-SUPTI-TIC-140-013-Segurança nas Comunicações
INP-SUPTI-TIC-140-014-Aquis Desenv Manut Software
INP-SUPTI-TIC-140-015-Fornecedores e Suprimentos
INP-SUPTI-TIC-140-016-Incidentes de Segurança da Informação
INP-SUPTI-TIC-140-017-Gestão da Continuidade de Negócio
INP-SUPTI-TIC-140-018-Conformidades

**NORMATIVOS REVOGADOS**

IN-SUPTI-TI-140 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TI-050 - Gestão de Ativos de TIC
TI-060 - Utilização de Recursos de TIC
TI-070 - Classificação da Informação
TI-080 - Controle de Acesso
TI-090 - Segurança Física
TI-100 - Política de Operações e Comunicações de Segurança da Informação
TI-110 - Gerir Processo de Software

**INSTÂNCIA DE APROVAÇÃO**

CONSELHO DE ADMINISTRAÇÃO DA SPA, 615ª REUNIÃO REALIZADA EM 13/05/2021, POR MEIO DA DELIBERAÇÃO CONSAD Nº 055.2021