MANUAL SGPI
USO ACEITÁVEL DE ATIVOS DE TIC

SUMÁRIO

MANUAL SGPI – USO ACEITAVEL DE ATIVOS DE TIC DA AUTORIDADE PORTUÁRIA DE SANTOS S.A.

1. DISPOSIÇÕES INICIAIS

Fica instituído o Manual do Sistema de Gestão de Privacidade da Informação (SGPI): Uso aceitável de Ativos de TI 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.

2. OBJETIVO E ABRANGÊNCIA

O presente Manual tem por objetivo definir as regras de utilização de recursos de TIC da SPA.

Este Manual é aplicado a todos os empregados, estagiários, menores aprendizes e prestadores de serviços.

3. DEFINIÇÕES

Para os fins deste Manual são adotados os seguintes conceitos:

Compartilhamento P2P: Peer-to-peer (do inglês par-a-par ou simplesmente ponto a ponto) ou P2P é uma arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

Malware: Programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros softwares.

"Malware" é um termo geral utilizado para se referir a uma variedade de formas de software hostil ou intruso.

Mídia: Termo utilizado neste manual para designar dispositivo de armazenamento de informações em sua forma digital (arquivos em seus diversos formatos inclusive áudio e vídeo). O dispositivo pode estar instalado fisicamente no interior de um equipamento (ex. HDs internos, SSDs internos) ou removível, acessível externamente ao equipamento podendo ser desconectado do equipamento e transportado (ex. HD removível ou externo, Pen drive, disco de CD/DVD, etc).

4. USO DOS ATIVOS DE TIC

4.1. A liberação ao uso dos ativos de TIC está condicionada à assinatura do Termo de Ciência de Confidencialidade e Sigilo Individual, conforme anexo I.

4.2. A instalação de qualquer tipo de software, ferramenta ou programa nos ativos de TIC pertencentes à SPA é atribuição exclusiva da Supervisão de Operação e Soluções de TI (SEOTI) e não deve ser executada sem acompanhamento desta.

4.3. Os ativos de TIC da SPA **não podem** ser utilizados para acessar, armazenar ou disponibilizar informações que contenham conteúdo das categorias abaixo, ou que se assemelhem a:

- Softwares (aplicativos, sistemas, utilitários) que não foram previamente homologados (testados e aprovados) pela TI, para apoio aos processos de negócios da SPA;
- Arquivos de áudio, vídeo ou imagens que possuam qualquer proteção de propriedade intelectual sem o devido respaldo legal por parte do proprietário;

- Pornografia, erotismo e pedofilia;
- Apologias ao terrorismo e às drogas;
- Violência e agressividade (racismo, preconceito, etc.);
- Jogos de computador;
- Jogos de apostas;
- Redes Sociais (Instagram, Facebook, etc.);
- Violação de sistemas de segurança;
- Violação de direito autoral (pirataria, etc.);
- Compartilhamento P2P de arquivos (uTorrent, bitTorrent e similares);
- Sites e ferramentas de redirecionamento de Proxy (Kproxy, YourFreedom e similares);

4.4. **Não será permitido** o uso de meios de comunicação que não possuam o nível de segurança adequado, definido pela SPA, para a transmissão de informações sensíveis de clientes e/ou parceiros.

4.5. A homologação de qualquer software de TI para apoiar um processo de negócio deve iniciar com o preenchimento de um Documento de Oficialização de Demanda (DOD), conforme modelo disponibilizado pela Supervisão de Governança de TI (SEGTI).

4.6. A Superintendência de Tecnologia da Informação (SUPTI) tomará as providências cabíveis caso seja detectado qualquer tipo de software malicioso, por exemplo, malwares, vírus, cracker, dentre outros, em qualquer estação de trabalho, devendo o usuário colaborar com a liberação imediata do ativo para investigação.

4.7. A identificação de qualquer ameaça ou caso confirmado de infecção por software malicioso deve ser comunicado imediatamente ao suporte de TI.

4.8. O dano gerado por mau uso dos equipamentos é passível de punição e ressarcimento, considerando, mas não se limitando, aos seguintes casos:

- Descuidos como, quedas, derrubada de comida, bebida ou produtos químicos e acúmulo de sujeira.
- Atos de violência como, socos, choques e arremessos.
- Alterações e instalações não autorizadas, como troca de peças, instalação de componentes ou ligação do equipamento em voltagem incompatível.
- Contaminação via malware/vírus por acesso indevido a páginas suspeitas ou por instalação de softwares não autorizados.
- Vazamento de informações sigilosas, incluindo dados pessoais.

4.9. O empréstimo de ativos da SPA que são de posse exclusiva do usuário **não é recomendado**. Ressarcimentos e punições em casos de mau uso por terceiros poderão ser de responsabilidade do usuário que emprestou o equipamento.

5. PROTEÇÃO DAS INFORMAÇÕES

São deveres do usuário de recursos de TI da SPA:

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

5.2. 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;

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

5.4. não tentar obter acesso à informação cujo grau de sigilo não seja compatível com o que possui na Companhia ou que não tenha autorização ou necessidade de conhecer;

5.5. não se passar por outro usuário usando ardilosamente sua identificação de acesso e senha;

5.6. não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de seu uso;

5.7. 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 teve acesso e não os divulgar a pessoas não autorizadas;

5.8. não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação

6. E-MAIL CORPORATIVO

6.1. A criação de e-mail corporativo do empregado deverá ser solicitada pelo superior imediato da Unidade de Gestão, por meio do sistema de chamados de TI.

6.2. A criação de e-mail setorial está condicionada a disponibilidade de contas e será solicitada e justificada pela Unidade de Gestão por meio do sistema de chamados de TI.

7. USUÁRIOS DO SERVIÇO DE E-MAIL CORPORATIVO

7.1. O acesso ao e-mail corporativo será realizado via aplicativo desktop Outlook ou via webmail (através de um navegador web).

7.2. A necessidade de configurações em outros dispositivos não contemplados deverá ser solicitada por meio do sistema de chamados de TI.

7.3. O usuário do e-mail corporativo:

- Será o único responsável pela administração de sua caixa de e-mail;
- Evitará o acúmulo de mensagens e arquivos inúteis;
- Respeitará o limite de espaço de cada caixa de correio.

7.4. A conta de e-mail é pessoal e intransferível e não pode ser compartilhada pelo usuário titular.

7.5. Na ausência do usuário titular deverá ser utilizada ferramenta de delegação para uso ou redirecionamento.

7.6. Ao se ausentar do ambiente de trabalho, o usuário encerrará a página de e-mail ou cliente de e-mail para evitar o acesso indevido.

7.7. O uso do e-mail corporativo não é tolerável para fins particulares e está sujeito a análises e verificações, não havendo privacidade do seu conteúdo.

7.8. Em relação às caixas de correio eletrônico das contas de e-mail corporativo, a SPA se reserva o direito de acessar, monitorar inclusive as respectivas mensagens com as seguintes finalidades, não se restringindo à:

- Identificação de *Malwares*, *Spams*, e outros códigos maliciosos similares;
- Urgência Comercial;
- Atividades de Investigação;
- Necessidade de suporte técnico para revisar o conteúdo das comunicações de membros individuais durante a resolução de problemas e/ou incidentes.

7.9. Todos os usuários de e-mail corporativo no domínio @portodesantos.com.br ou @brssz.com:

- Estarão cientes de que todas as mensagens enviadas detêm a marca SPA; e,
- Serão diretamente responsáveis por seu conteúdo.

7.10. A mensagem enviada a partir de uma conta setorial, deve contar, ao final, com a identificação do usuário remetente, sendo este corresponsável pela informação prestada junto à sua chefia imediata.

7.11. Recomenda-se a utilização de assinatura padrão conforme estabelecido no Manual de Marca Porto de Santos Vigente, acrescido do texto:

"Esta mensagem pode conter informações confidenciais e/ou privilegiadas. Se não for o seu destinatário, favor comunicar imediatamente ao remetente e destruir todas as informações e suas cópias".

“This message may contain confidential and / or privileged information. If it is not the intended recipient, please notify the sender immediately and destroy all information and copies".

7.12. Toda mensagem de correio eletrônico deverá ser redigida e enviada de maneira profissional, seguindo todas as normas e práticas de decoro social.

7.13. **Não é permitido** fazer uso do serviço de e-mail corporativo para expor opiniões pessoais a terceiros nem falar mal de algo ou de alguém.

7.14. É boa prática atentar-se para o uso da função de encaminhamento de e-mails ou informações para outras pessoas/entidades, evitando-se quando possível.

7.15. Recomenda-se que o encaminhamento seja autorizado pelo remetente da mensagem de correio eletrônico original.

7.16. **É proibido** o encaminhamento automático de mensagens de e-mail para e-mails externos, como por exemplo e-mails pessoais.

7.17. **É proibido** o cadastro do e-mail corporativo, próprio ou setorial, em sites de terceiros, exceto naqueles que estabeleçam interesses institucionais, como exemplo: CNPq, ENAP e outros órgãos públicos.

7.18. **É proibido** o cadastro do e-mail corporativo, próprio ou setorial, em sites de terceiros que forneçam bens e serviços, inclusive aplicativos e/ou sistemas, exceto aqueles que a SPA oficialmente mantenha algum vínculo (de preferência contratual) ou haja a devida autorização para tal.

7.19. Considerar fazer uso de ferramentas de compactação de arquivos ou arquivos com formato reduzido (.zip, .rar, .pdf, etc.) para o envio de e-mails.

7.20. **Não devem** ser respondidos ou abertos e-mails e nem seus anexos:

- de remetente desconhecido; e
- de caráter ou conteúdo duvidoso.

7.21. Notificar à Superintendência de Tecnologia da Informação (SUPTI) via SEOTI, por chamado de TI, sobre qualquer comportamento suspeito no serviço de correio eletrônico.

8. INFORMAÇÃO EM MÍDIA

8.1. Dispositivos USB **são bloqueados** por padrão, pois seu uso de forma indiscriminada é uma enorme porta de entrada para "malwares" (vírus) e traz riscos de segurança cibernética para a SPA, sendo assim, o controle

da utilização de tais dispositivos, reduz a incidência de entrada de "malwares" na companhia.

8.1.1. A liberação será dada mediante solicitação formal do gestor imediato do empregado, via sistema de chamados de TI, e que, se autorizado, deverá ser declarada e registrada a ciência e responsabilidade da utilização, tanto pelo empregado como pelo gestor imediato no que diz respeito às demais diretrizes da seção 8. Informação em Mídia desse manual.

8.2. **É proibida** a gravação em mídias removíveis de:

- Arquivos que desrespeitem a ética corporativa e/ou legislação;
- Programas, sistemas e/ou softwares que sejam de propriedade da SPA (desenvolvidos internamente e/ou por ela comprados).

8.3. As mídias removíveis, quando autorizadas para uso, deverão ser utilizadas apenas para a transferência de informações de negócio.

8.4. O uso de mídias removíveis está condicionado ao compromisso do usuário em:

- usufruir devidamente destas mídias;
- não revelar ou divulgar informações armazenadas em seu interior, definidas como não públicas pela SPA, inclusive após o término de seu vínculo contratual.
- se responsabilizar por quaisquer danos, diretos ou indiretos, presentes ou futuros, pelo mau uso ou uso indevido, que venham a causar à SPA e/ou a terceiros.

8.5. Mídias removíveis desconhecidas, inclusive e principalmente, aparelhos celulares, **não devem** ser conectados em computadores da companhia.

8.6. Todo dado ou informação sem necessidade de uso será descartado por meio de:

- remoção completa da mídia (seguindo as melhores práticas existentes); ou
- destruição física da mídia (quando não for possível apagar as informações).

8.7. O descarte de informações relacionadas aos sistemas de informação (manuais, descritivos, tabelas, relatórios etc.), deve seguir os requerimentos desse Manual.

9. USO DA INTERNET CORPORATIVA

9.1. O uso da Internet corporativa é autorizado para fins particulares, desde que não comprometa as atividades do empregado e que não confronte qualquer item deste Manual.

9.2. Todos os acessos são monitorados e registrados (*logs*) para posterior consulta, visando o atendimento das diretrizes de segurança da rede.

10. TELEFONES FIXOS, CELULARES E RÁDIOS

10.1. É prudente evitar tratar de assuntos profissionais e/ou de caráter confidencial com ou sem o uso de meios de comunicação (telefones celulares, radiocomunicadores e similares), em ambientes ou locais públicos tais como restaurante, transporte público, táxi, etc.

10.2. O empregado **não pode** criar, gravar ou manter mensagens com informações sensíveis em serviços de secretárias eletrônicas de clientes e parceiros.

11. DISPOSITIVOS MÓVEIS PRÓPRIOS (*BRING YOUR OWN DEVICE* - BYOD)

11.1. É facultativo ao empregado o uso de dispositivo próprio para suas tarefas cotidianas, desde que esse dispositivo:

- seja legalmente licenciado incluindo o software de Sistema Operacional e demais aplicativos executados no dispositivo.
    - O licenciamento desses, softwares próprios ou de terceiros que venha a utilizar para a execução de suas tarefas, é de responsabilidade do empregado.
- tenha proteção ou nível de segurança equivalente ao adotado para os ativos da SPA.

NOTA.: O uso indevido e/ou ilegal de software é passível de responsabilização ao empregado por qualquer incidente de pirataria.

11.2. O acesso a rede de dados a partir de um dispositivo próprio atenderá, no mínimo, aos seguintes requisitos de segurança:

- Ter aprovação formal (física ou digital) de seu superior (Gerente, Superintendente ou Diretor);
- Assinar o Termo de Ciência e Responsabilidade;
- Atender aos requisitos mínimos de sistemas aprovados pela Gerência de Infraestrutura de Dados (GERID); e,
- O dispositivo tem de:
    - possuir um antivírus ativo;
    - estar devidamente cadastrado na rede da SPA pela GERID;
    - estar atualizado quanto aos *patches* de segurança;
    - Ser de uso exclusivo do empregado e não compartilhado com outras pessoas alheias à atividade do empregado na SPA.

É passível de cancelamento do acesso por equipamento próprio à rede corporativa da SPA, quando ocorrer o descumprimento, em todo ou em parte, dos itens acima.

11.3. É de responsabilidade do empregado a manutenção e guarda de equipamento próprio, arcando com qualquer ônus causado por perda, deterioração, furto, extravio ou avaria que venha a acontecer, bem como perda de conteúdo armazenado. Na ocorrência de um dos eventos citados acima, o usuário deverá comunicar imediatamente à GERID para que sejam adotadas as medidas cabíveis em relação à segurança e à privacidade das informações da SPA.

11.4. O *backup* (cópia de segurança) de todos os dados, pessoais e empresariais, armazenados no dispositivo é de responsabilidade e será realizado pelo próprio usuário.

11.5. O armazenamento de dados corporativos deve ser sempre efetuado na própria rede interna da SPA e nos recursos de rede disponibilizados pela SPA, inclusive armazenamento em nuvem contratado pela SPA.

11.6. Todo equipamento que armazene dados corporativos deve ser transportado com a máxima discrição e zelo, a fim de evitar:

- acidentes,
- furtos,
- roubos e/ou vazamento de informações sensíveis.

11.7. **Não é recomendado** o acesso aos recursos da SPA armazenados em serviços de nuvem (ex. Office 365) por meio de dispositivos que não sejam da SPA ou do empregado, também não é recomendado o acesso em locais públicos (ex. Lan House, Cybercafé, Internet Pública de aeroportos, e locais similares).

12. GESTÃO DO EQUIPAMENTO PELA SPA

12.1. A SPA, ostensivamente, reserva-se ao direito de gerenciar fisicamente apenas os equipamentos fornecidos pela Companhia, considerando as

instruções contidas no presente Manual, bem como para mitigação de riscos.

12.2. A SPA, ostensivamente, reserva-se ao direito de monitorar logicamente todo e qualquer equipamento que venha a fazer parte de sua rede, a fim de mitigar qualquer risco de acesso lógico das informações.

12.3. É facultativo à SPA apagar remotamente dados sensíveis e sigilosos em equipamentos próprios ou de terceiros, quando constatado a ocorrência de risco à segurança e à privacidade de dados em caso de roubo, perda ou cometimento de transgressão disciplinar.

12.4. A SPA pode, a qualquer momento, retirar ou substituir os equipamentos concedidos à usuários, podendo estar entre os motivos:

- troca de setor ou função;
- atualização Tecnológica;
- desligamento;
- auditorias de Segurança.

13. SUPORTE AO EQUIPAMENTO

13.1. Em qualquer evento de problema ou incidente referente aos ativos de TIC da SPA, deverá ser requisitada a assistência técnica por meio da abertura de chamados junto à SEOTI.

13.2. Caso o usuário necessite de suporte em seu equipamento pessoal, a SEOTI se resguarda ao direito de limitar o suporte quanto às funcionalidades necessárias para acesso ao ambiente de rede da SPA.

13.3. **Não configura** obrigação de atendimento pela SEOTI sob a constatação de:

- mau funcionamento do ativo por uso indevido de hardware particular do requisitante;

- que o equipamento não está relacionado ao negócio.

14. USO DE SENHAS

14.1. São medidas de segurança no uso de senha:

- Não permitir que outros empregados ou terceiros a vejam enquanto digita;
- Não compartilhar a senha com outra pessoa;
- Não deixar a senha grafada em local visível para outros empregados ou terceiros;
- Não permitir o desbloqueio automático de computadores em caso de início de sessão;
- Não salvar automaticamente a senha em nenhum equipamento, software ou recurso remoto.
- Não utilizar senha com sequência fácil ou óbvia de caracteres que facilite a sua descoberta.

14.2. É necessário adotar o padrão de senhas especificado no Instrumento Normativo "INP-SUPTI-TIC-140-009-Gestao de Acesso" para utilização onde aplicável de ativos de TI, tanto para uso comum como para fins de administração do ativo.

14.3. A criação de usuários e senhas de serviços só ocorrerá com a aprovação prévia da GERID.

15. MESA LIMPA/TELA LIMPA

15.1. O usuário **não deve** deixar o Laptop/Notebook em sua mesa fora do horário de trabalho, exceto se estiver protegido por um cabo de aço com cadeado.

15.2. O usuário sempre bloqueará o dispositivo/terminal/ativo contra uso indevido quando se ausentar de seu local de trabalho, utilizando o conjunto de teclas apropriados ao dispositivo. Ex (microcomputadores): CTRL+ALT+DELETE seguido de ENTER ou WINDOWS + L.

15.3. Qualquer impressão, fax ou correspondência tem que ser recolhido imediatamente pelo empregado, a fim de evitar que informações sensíveis impressas sejam acessadas indevidamente.

15.4. É boa prática que alimentos e bebidas não estejam nas estações de trabalho, a fim de proteger as informações e os ativos da Companhia.

16. ACESSO REMOTO E TELETRABALHO

16.1. O acesso remoto às redes da SPA, por meio de dispositivos móveis próprios (considerando os requisitos de dispositivos móveis próprios), ou não, encontram-se restritos apenas a empregados autorizados por meio de mecanismos com objetivo de garantir a segurança no acesso. Caso o mecanismo exija a instalação de componente específico e o mesmo não puder ser instalado, independente do motivo, o acesso remoto não será permitido.

16.2. É facultativo ao usuário o acesso remoto à rede da SPA por meio de dispositivo próprio em qualquer dia e horário, entretanto esse acesso não caracteriza sobreaviso ou sobre jornada.

16.3. O empregado que esteja autorizado a usar as facilidades de acesso remoto à SPA, protegerá adequadamente sua estação de trabalho para evitar acesso não autorizado, em especial de pessoas com acesso físico ao equipamento (ex.: parentes e amigos), ficando cada usuário pessoalmente responsável pela proteção de sua estação de trabalho e uso correto das facilidades as quais possui autorização de uso.

17. DISPOSIÇÕES FINAIS

17.1. Os casos omissos no presente Manual devem ser analisados pela SUPTI.

17.2. A não observância deste Manual implicará, no que couber, em sanções previstas no Regulamento Interno de Pessoal e/ou no Código de Ética da SPA, além de outras responsabilizações eventualmente aplicáveis.

INFORMAÇÕES DE CONTROLE

TÍTULO

MANUAL SGPI USO ACEITÁVEL DE ATIVOS DE TIC

VERSÃO

1.1.2

UNIDADE GESTORA DO DOCUMENTO

Superintendência de Tecnologia da Informação

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

Adição de parágrafos;

Adição do tópico: 5. PROTEÇÃO DAS INFORMAÇÕES;

Exclusão de parágrafos.

RELAÇÃO COM OUTROS NORMATIVOS

Política de Segurança e Privacidade e SGPI;

Regulamento Interno de Pessoal da SPA.

Código de Ética e de Conduta e Integridade;

Instrumento Normativo Sistema de Gestão Da Privacidade da Informação: Gestão de Ativos.

NORMATIVOS REVOGADOS

N/A

INSTÂNCIA DE APROVAÇÃO

PRESIDENTE DA SPA, EM 16/02/2022, POR MEIO DO DOCUMENTO SDD Nº 69713/2021.

ANEXO I – TERMO DE CIÊNCIA DE CONFIDENCIALIDADE E SIGILO INDIVIDUAL

TERMO DE CIÊNCIA DE CONFIDENCIALIDADE E SIGILO INDIVIDUAL

Eu, _____, portador(a) do CPF / Registro nº _____, perante a Santos Port Authority (Autoridade Portuária de Santos), doravante denominada SPA, na qualidade de usuário ou prestador de serviços do ambiente computacional de propriedade da referida Companhia e/ou tendo a possibilidade ou condição de acesso direto às informações da mesma, declaro que estou ciente das diretrizes de Segurança da Informação da SPA e recebi cópia/orientações de acesso às normas relacionadas a minha função.

No âmbito da SPA, assumo os compromissos de:

1. cumprir as determinações normativas de Segurança da Informação e tomar ciência de suas atualizações nos canais corporativos de comunicação;
2. não utilizar, copiar e divulgar informações sigilosas (confidenciais e secretas) com propósito que não seja de meu escopo de trabalho;
3. me responsabilizar e zelar pelos ativos da SPA sob minha posse e custódia, não acessando conteúdos indevidos, utilizando softwares não autorizados e prevenindo danos ocasionados por mau uso;
4. ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de mau uso dos equipamentos, ou uma eventual quebra de sigilo das informações fornecidas, provocada por ato doloso ou erro grosseiro, sem prejuízo de responsabilidade criminal;
5. não efetuar o tratamento de dados pessoais além do que contemplar e/ou instruir a Autoridade Portuária de Santos através dessa relação e dentro do respectivo objeto;
6. informar o suporte de TI a respeito de qualquer suspeita ou caso de ameaça de vazamento de informações sigilosas;
7. devolver os equipamentos da SPA em casos como atualizações, suspeitas de ameaças, transferências de setor e desligamento da empresa;

A **vigência** da obrigação de confidencialidade e sigilo, assumida pela minha pessoa por meio deste termo, terá validade de 6 meses após encerramento de meu vínculo contratual com a Autoridade Portuária de Santos ou uma de suas Contratadas para Prestação de Serviços.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Sigilosa informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade, do Estado e do Negócio da Empresa, e aquela abrangida pelas demais hipóteses legais de sigilo.

Informações Pessoais/Dados Pessoais: são aquelas relacionadas a uma pessoa natural identificada ou identificável, em qualquer formato de armazenamento (papel, arquivos digitais, imagens, etc.) e sujeitos a confidencialidade e sigilo do presente Termo

O subscrito obriga-se a cumprir o presente termo de confidencialidade e sigilo sob pena de responsabilidade civil e criminal, considerando as exceções previstas na "Política de Segurança e Privacidade e SGPI", bem como as limitações de cumprimento do presente termo advindas de adequações em curso (de procedimentos, de Sistemas de Informação, etc), para atendimento à "Política de Segurança e Privacidade e SGPI".

_____

Santos, XX de XXXXX de 20XX

[Nome Funcionário]
[Cargo]
[Razão Social da Empresa]

SANTOS PORT AUTHORITY

TERMO DE CIÊNCIA DE CONFIDENCIALIDADE E SIGILO INDIVIDUAL

ORIENTAÇÕES

A SPA possui uma Política de Segurança e Privacidade, e Sistema de Gestão de Privacidade da Informação e um conjunto de normas derivadas que trazem diretrizes sobre como as informações, principalmente as sigilosas e pessoais, devem ser protegidas. Este conjunto de normas é redigido pelo setor de Segurança da Informação e aprovado pelo Comitê de Segurança da Informação, tratando, de forma abrangente, mas não se limitando, de temas como: proteção física e lógica das informações (criptografia, senhas, restrições de acesso, etc.), comportamentos esperados pelos usuários e métodos de registro e acompanhamento de ameaças e vulnerabilidades.

Os normativos podem ser encontrados na seção de documentos da Intranet da SPA, com o termo "SGPI" ou "Sistema de Gestão da Privacidade da Informação" sendo utilizado na busca. Caso não tenha acesso à Intranet, também é possível acessá-los no site do porto, através do endereço https://portodesantos.com.br/SGPI.

Além disso existe uma cartilha de utilização dos recursos de TI, com proposta de guia rápido de consulta, mais amigável para usuários, esta pode ser encontrada na seção de Downloads/Manuais e Apostilas da Intranet da SPA ou no mesmo link citado acima.

A seguir, listagem de normativos que devem ser de sua ciência de acordo com o seu papel exercido:

NECESSIDADE DE CIÊNCIA EM NORMATIVOS DE SEGURANÇA DA INFORMAÇÃO			
NORMA DE SI	**FUNCIONÁRIOS SPA[1]**	**PRESTADORES DE SERVIÇO**	**FUNCIONÁRIOS DE TI**
Política de Segurança e Privacidade, e Sistema de Gestão de Privacidade da Informação	⚠ **obrigatória**	⚠ **obrigatória**	⚠ **obrigatória**
Manual de uso aceitável de ativos de TI	⚠ **obrigatória**	⚠ **obrigatória**	⚠ **obrigatória**
Outros normativos de SI	👍 **recomendada**	⚠ **obrigatória**	⚠ **obrigatória**
Cartilha de utilização de recursos de TI	👍 **recomendada**	👍 **recomendada**	👍 **recomendada**

[1] Engloba concursados, cargos de livre provimento, conselheiros, estagiários e aprendizes