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., "APS" 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 APS.

Este Manual é aplicado a todos os empregados, estagiários, menores aprendizes e prestadores de serviços, que deverão zelar e tomar todos os cuidados necessários para manter o bom funcionamento de qualquer equipamento colocado a sua disposição pela APS para uso durante o desempenho de suas atividades

3. DEFINIÇÕES

Para os fins deste Manual são adotados os seguintes conceitos:

Central de Serviços/Central de Serviços de TI: é um ponto único de contato (Single Point of Contact - SPOC) entre a área de TI e os usuários de recursos de TI, através do qual a TI é solicitada para atender demandas de TI.

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, funcionam tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.**Documento de Oficialização de Demanda (DOD):** Documento que oficializa a intenção ou registra a necessidade de um produto ou serviço para atender a uma

demanda em função uma atividade nova ou aprimoração de uma existente, ou requisito. É o ponto inicial para que o recurso seja providenciado através de uma aquisição ou outro processo que possa atender a demanda. Vide.....

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).

Roaming: capacidade do aparelho celular obter conectividade em áreas fora da localidade geográfica onde está registrado (ex.: DDD 013), ou seja, obtendo conectividade através de uma outra rede (ex. de rede: DDD 013) onde é visitante. A rede que está sendo visitada pode ou não pertencer à mesma operadora;

Smartphones: aparelho de telefone celular com funcionalidades avançadas que podem ser entendidas por meio de programas executados no seu sistema operacional;

Software Malicioso: Vide Malware;

TIC: Tecnologia de Informação e Comunicação.

4. USO DOS ATIVOS DE TIC

4.1. A liberação ao uso dos ativos de TIC da APS está condicionada à assinatura do Termo de Ciência de Confidencialidade e Sigilo Individual, conforme anexo I. No caso de empregados de empresas contratadas pela APS o Termo deve ser preenchido sem o logo da APS.

4.2. A liberação para uso dos ativos de TIC da APS, com características de mobilidade (dispositivos móveis, ex.:rádios, laptops, celulares, etc), está condicionada a assinatura de termos específicos (vide Item “Aparelhos Celulares Corporativos” e Anexo VI para laptops) ou Recibos de entrega de equipamentos e acessórios.

4.3. A instalação de qualquer tipo de software, ferramenta ou programa nos ativos de TIC pertencentes à APS é atribuição exclusiva da central de serviços e não deve ser executada sem acompanhamento desta.

4.4. Os ativos de TIC da APS **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 APS;
- 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.), a não ser que estritamente vinculado a rotina de trabalho;
- Violação de sistemas de segurança e suas proteções, tanto da APS como de terceiros;
- Violação de direito autoral (pirataria, etc.);
- Compartilhamento P2P de arquivos (uTorrent, 6ivulga6nt e similares);
- Sites e ferramentas de redirecionamento de Proxy (Kproxy, YourFreedom e similares);

4.5. **Não será permitido** o uso de meios de comunicação (através dos ativos de TI) que não possuam o nível de segurança adequado, definido pela APS, para a transmissão de informações sensíveis de clientes e/ou parceiros. Orientações poderão ser solicitadas à GERID via sistema de chamados de TI.

4.6. A homologação de qualquer software de TI para apoiar um processo de negócio deve:

4.6.1. Ter uma avaliação, cujo processo coordenado pela GERID, envolve a consulta a outros setores conforme a necessidade e de acordo com funções e normas vigentes, ou

4.6.2. iniciar com o preenchimento de um Documento de Oficialização de Demanda (DOD), conforme orientação dada após avaliação do chamado aberto e modelo disponibilizado pela Supervisão de Governança de TI (SEGTI).

4.7. A GERID 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. A providências serão dadas conforme INP-Gestão de Serviços de TIC, subprocesso gestão de incidentes de SI&P e o Regulamento Interno de Pessoal.

4.8. A identificação de qualquer suspeita ou caso confirmado de infecção por software malicioso deve ser comunicada imediatamente à central de serviços de TIC através de chamado.

4.9. O dano gerado por mau uso dos equipamentos é passível de punição e ressarcimento, de acordo com o previsto nos normativos “MANUAL DE PROCEDIMENTOS DE IDENTIFICAÇÃO E RESPONSABILIZAÇÃO POR DANOS CAUSADOS POR EMPREGADO AO PATRIMÔNIO DA APS E/OU SOB SUA RESPONSABILIDADE” e “MANUAL DE CONDUTA E INTEGRIDADE”, 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.

4.10. O empréstimo de ativos da APS 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 APS:

5.1. tratar a informação digital como patrimônio da APS 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 APS 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, ou sistemas não relacionados com a atividade, ou ferramentas de inteligência artificial que não estejam sob controle da APS;

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 decorrer do processo de desligamento ou afastamento, seja por exoneração, demissão, licenciamento, término de prestação de serviço, é necessário que o colaborador preserve o conteúdo das informações e documentos sigilosos, evitando, dessa forma, o descarte ou a divulgação a pessoas não autorizadas;

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

5.9. no caso de uso de ferramentas de Inteligência Artificial, não alimentar com informações sigilosas, restritas ou pessoais, e responsabilizar-se pelos resultados fornecidos pela ferramenta, revisando-os sempre.

6. USUÁRIOS DO SERVIÇO DE E-MAIL CORPORATIVO

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

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

6.3. 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.

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

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

6.6. O usuário ao se ausentar do ambiente de trabalho ou do posto de trabalho deverá adotar ações para evitar o acesso e utilização indevida do e-mail, em consonância com as regras descritas no item “Mesa Limpa/Tela Limpa” desse manual, ou seja, bloquear o dispositivo de forma que somente seja desbloqueado mediante nova autenticação.

6.7. 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.

6.8. Em relação às caixas de correio eletrônico das contas de e-mail corporativo, a APS 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.

6.9. Em caso de desligamento do usuário da conta de e-mail, a respectiva conta será desabilitada da mesma forma que as demais contas de acesso (ex.: acesso à sistemas, intranet, etc). A correspondente caixa de correio poderá ser disponibilizada ao superior imediato ou substituto, para fins de, porém não limitado à, continuidade de assuntos de interesse da APS tratados pelo desligado, resguardando-se as restrições de envio pela conta do desligado.

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

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

6.11. É recomendado que haja identificação do usuário remetente do e-mail quando uma conta setorial é utilizada. Cabe à área de negócio gestora da conta setorial a decisão

de realizar ou não essa identificação. A decisão tomada não prejudica que, por questões de segurança, haja rastreabilidade por outros meios de qual usuário está enviando a mensagem.

6.12. Recomenda-se a utilização de assinatura padrão conforme estabelecido no Guia rápido de uso da Marca, 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".

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

6.14. **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.

6.15. Recomenda-se que mensagens que não devam ser encaminhadas sejam indicadas pelo remetente. A indicação pode ser feita de forma taxativa no corpo do e-mail, ou a partir de opções no aplicativo que impeçam o encaminhamento.

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

6.17. **Não é permitido** que se use o e-mail corporativo para o cadastro em sites/serviços que não tenham relação com as atividades de trabalho. São exemplos de cadastros encarados como proibidos: serviços de streaming, lojas online, mídias sociais focadas para o entretenimento, jogos de azar, etc.

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

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

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

6.20. Notificar a Central de Serviços por chamado de TI, sobre qualquer comportamento suspeito no serviço de correio eletrônico.

7. INFORMAÇÃO EM MÍDIA REMOVÍVEL

7.1. As portas USB são **bloqueadas** por padrão, por ser uma porta de entrada para programas maliciosos.

7.1.1. A liberação de portas USB 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.

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

- transferir apenas informações necessárias para consecução de atividades;
- usufruir devidamente destas mídias;
- não revelar ou divulgar informações armazenadas em seu interior, definidas como não públicas pela APS, 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 APS e/ou a terceiros, conforme “MANUAL DE PROCEDIMENTOS DE IDENTIFICAÇÃO E RESPONSABILIZAÇÃO POR DANOS CAUSADOS POR EMPREGADO AO PATRIMÔNIO DA APS E/OU SOB SUA RESPONSABILIDADE” e “MANUAL DE CONDUTA E INTEGRIDADE”.

7.3. **É proibida** a conexão de mídias removíveis em computadores da Companhia, cuja origem seja desconhecida e/ou duvidosa, inclusive aparelhos celulares.

7.4. O descarte de mídias da empresa compete à GERID. Havendo necessidade, deve-se abrir um chamado junto à central de serviços de TIC.

8. USO DA INTERNET CORPORATIVA

8.1. 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.

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

9. TELEFONES FIXOS, CELULARES E RÁDIOS

9.1. 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.

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

9.3. Os procedimentos administrativos relativos à celulares de propriedade da APS, estão descritos no item “Aparelhos Celulares Corporativos” e os relativos a celulares e outros dispositivos particulares no item “Dispositivos Móveis Próprios”.

10. DISPOSITIVOS MÓVEIS PRÓPRIOS (*BRING YOUR OWN DEVICE* – BYOD)

10.1. 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 exclusiva do empregado.

- tenha proteção ou nível de segurança equivalente ao adotado para os ativos da APS.

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

10.2. **É vedado** o acesso à rede de dados e recursos da APS (servidores, sistemas, etc) partir de um dispositivo próprio. No entanto o acesso à internet poderá ser feito via rede apartada, indicada para essa finalidade. Exceções poderão ser consideradas, resguardadas os interesses da APS (ex.: consultores externos, auditores etc.), desde que em conformidade com requisitos de segurança.

10.3. O acesso a rede de dados a partir de um dispositivo próprio (ou de terceiros) atenderá, no mínimo, aos seguintes requisitos de segurança:

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

O acesso referido nessa diretriz pode ser cancelado em qualquer momento que ocorrer o descumprimento, em todo ou em parte, dos itens acima.

10.4. Recomenda-se que as informações da APS não sejam armazenadas em dispositivos próprios.

10.5. 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 que seja pertinente à APS. 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 APS.

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

10.7. 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.

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

11. GESTÃO DO EQUIPAMENTO PELA APS

11.1. A APS, 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.

11.2. A APS, 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.

11.3. É facultativo à APS, através da GERID utilizando dos recursos disponíveis, apagar dados remotamente de maneira preventiva 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 ato que possa incorrer em transgressão disciplinar.

11.4. A GERID 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.

11.5. Em casos de perda, roubo ou furto, informar imediatamente a GERID (em caso aparelho celular corporativo: Setor de Telecomunicações), por mensagem eletrônica, especificando o motivo e fato ocorrido;

11.6. Em casos de roubo e furto, deverá ser anexado o Boletim de Ocorrência na mensagem eletrônica enviada à GERID. Caso a ocorrência tenha sido em áreas da APS, deverá ser acionada a Guarda Portuária e lavrado um Registro de Ocorrência; Em casos de roubo e furto de aparelho celular corporativo, a GERID deverá providenciar o bloqueio da linha junto à operadora;

12. SUPORTE AO EQUIPAMENTO

12.1. Em qualquer evento de problema ou incidente referente aos ativos de TIC da APS, deverá ser requisitada a assistência técnica por meio da abertura de chamados de TI.

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

12.3. **Não configura** obrigação de atendimento pela GERID sob a constatação de:

- mau funcionamento do ativo por uso indevido de hardware particular do requisitante;
- que o equipamento não está relacionado ao negócio.

13. USO DE SENHAS

13.1. 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 transcrita 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.

13.2. É necessário adotar o padrão de senhas especificado no Instrumento Normativo de "Gestão de Serviços – Subprocesso: Gestão de Acessos Lógicos" para utilização onde aplicável, tanto para uso comum como para fins de administração de ativos e recursos.

14. MESA LIMPA/TELA LIMPA

14.1. 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.

14.2. O usuário **deve** bloquear o dispositivo/terminal/ativo contra uso indevido quando se ausentar de seu local de trabalho, utilizando o conjunto de teclas apropriados ao dispositivo, de modo que o desbloqueio só ocorra mediante uma nova autenticação. Ex (microcomputadores): CTRL+ALT+DELETE seguido de ENTER ou WINDOWS + L.

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

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

15. ACESSO REMOTO E TELETRABALHO

15.1. O acesso remoto às redes da APS, encontra-se restrito apenas a usuários 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.

15.2. Os impactos do acesso remoto à rede da APS nos controles de jornada e outros controles de recursos humanos estão previstos no MANUAL DE ORIENTAÇÕES AO TELETRABALHO.

15.3. O empregado que esteja autorizado a usar as facilidades de acesso remoto à APS, **deve** proteger 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.

16. APARELHOS CELULARES CORPORATIVOS

16.1. Os itens abaixo, visam disciplinar os procedimentos administrativos que deverão ser adotados para o uso do celular corporativo, recurso este disponibilizado para o trabalho que visa melhora a comunicação interna/externa.

16.2. DOS ELEGÍVEIS

- Anualmente será revisto o quantitativo de aparelhos celulares que se fará necessário na APS, bem como os empregados/setores elegíveis a usá-los, de acordo com a atribuição do setor ou da função do usuário;
- A Gerência de Infraestrutura de Dados (GERID) será responsável por realizar essa revisão verificando a necessidade de cada um dos aparelhos juntos aos gestores/responsáveis;
- Caso a GERID entenda que as justificativas não são suficientes, poderão requerer informações complementares, bem como negar a elegibilidade. Permanecendo a dúvida, poderão contatar à área de Gestão de Pessoas;
- A relação de elegíveis deverá ter caráter impessoal e considerar as atribuições a serem executadas;
- Não serão elegíves terceirizados, estagiários e os menores aprendizes;
- Não farão jus ao aparelho celular corporativo, empregados lotados em unidades administrativas que executam seus serviços internamente, ou seja, que podem valer-se dos aparelhos fixos;
- Deverão dispor de celulares próprios com acesso à Internet às custas do próprio empregado, os ocupantes de Cargos Comissionados (Superintendentes, Gerentes, Assessores, Secretárias e Gestor de VTMIS), conforme previsto no Contrato de Trabalho; e
- A elegibilidade dos usuários para o uso do aparelho celular poderá ser revista ou contestada a qualquer momento pela GERID ou pela área de Gestão de Pessoas,

para garantir o uso adequado e em conformidade com o propósito estabelecido, além da possibilidade de requisitar os aparelhos para remanejamentos ou outras necessidades pertinentes, sem prejuízo às atividades que dependam desse recurso.

16.3. DOS APARELHOS CORPORATIVOS

- Os aparelhos fornecidos pela APS serão aqueles previstos em Contrato de prestação de serviços de telefonia móvel.

16.4. DOS CONTROLES (INÍCIO E TÉRMINO)

- Os empregados elegíveis ao uso do aparelho celular corporativo deverão assinar o "Termo de Responsabilidade Telefone Celular Corporativo" (anexo II deste Manual);
- Caso o empregado negue-se a firmar o "Termo de Responsabilidade Telefone Celular Corporativo", o aparelho não poderá ser entregue;
- Caso o empregado se negue a utilizar o celular corporativo, optando pela utilização de seu próprio aparelho e linha, deverá firmar "Termo de Recusa do Celular Corporativo" (anexo IV deste Manual);
- Caso o empregado opte por utilizar apenas o chip, valendo-se de seu próprio aparelho celular, deverá incluir no campo observação do "Termo de Responsabilidade Telefone Celular Corporativo" (anexo II deste Manual) que "opto, voluntariamente, em utilizar meu próprio aparelho celular";
- O empregado deverá devolver o telefone celular corporativo, quando solicitado, no prazo de 24 (vinte quatro) horas. Caso não seja respeitado, a GERID notificará a Superintendência de Tecnologia da Informação (SUPTI) para providências cabíveis;
- Em caso de desligamento, o empregado deverá entregar o equipamento corporativo diretamente à GERID ou ao seu Gestor que, neste caso, deverá providenciar a devolução à GERID;
- Quando da devolução de equipamento corporativo deverá ser firmado o "Termo de Devolução Telefone Celular Corporativo" (anexo III deste Manual);

- Caso seja verificado algum extravio no aparelho corporativo a GERID deverá notificar a SUPTI para providências cabíveis; e
- Os TERMOS deverão ser arquivados na Pasta Individual dos empregados do RH.

16.5. DA CLONAGEM DE LINHAS

- Caso o empregado suspeite que sua linha foi clonada, este deve informar imediatamente a GERID pelo Sistema de Chamados de TI. Caberá à GERID tomar as providências junto a operadora celular.

16.6. DISPOSIÇÕES GERAIS

- Não é permitido ao usuário trocar, vender, ou repassar o aparelho para terceiros. É também proibida a habilitação de serviços adicionais à linha, ou mesmo transferir o número para um celular particular;
- Não será possível a utilização da linha móvel fora do Brasil;
- O uso do aparelho celular corporativo é estritamente para fins laborais concernentes à APS; e
- Os casos omissos relativos à “Aparelhos Celulares Corporativos” serão deliberados pelo Superintendente de Gabinete da Presidência (SUGAB) e, em segunda instância, pelo Presidente da APS.

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 APS, além de outras responsabilizações eventualmente aplicáveis.

ANEXO I – TERMO DE CIÊNCIA DE CONFIDENCIALIDADE E SIGILO, INDIVIDUAL

Eu, _____, portador(a) do CPF / Registro nº _____, perante a Autoridade Portuária de Santos, doravante denominada APS, 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 APS e recebi cópia/orientações de acesso às normas relacionadas a minha função.

No âmbito da APS, 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 APS 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 APS 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]

ORIENTAÇÕES

A APS 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 APS 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

ANEXO II – TERMO DE RESPONSABILIDADE TELEFONE CELULAR CORPORATIVO

Pelo presente responsabilizo-me pela guarda e posse do chip e/ou aparelho relacionado abaixo, respondendo perante APS em caso de furto, roubo, extravio ou semelhante, bem como pela má utilização ou qualquer dano causado ao bem, conforme "MANUAL DE PROCEDIMENTOS DE IDENTIFICAÇÃO E RESPONSABILIZAÇÃO POR DANOS CAUSADOS POR EMPREGADO AO PATRIMÔNIO DA APS E/OU SOB SUA RESPONSABILIDADE" e "MANUAL DE CONDUTA E INTEGRIDADE" comprometendo-me a prestar os devidos esclarecimentos por escrito à GERID na ocorrência de qualquer dos eventos acima.

Comprometo-me, ainda, a utilizá-lo de forma estritamente funcional, obrigando-me a devolvê-lo em perfeito estado de conservação em caso de exoneração do cargo ou quando solicitado pela unidade responsável pelo equipamento.

Após conferir e estar de acordo, declaro que recebi o chip e/ou aparelho relacionado e que o mesmo está em perfeita condição de uso.

ENTREGA

( ) CHIP – Operadora: _____ Núm. Linha: (13) _____

( ) APARELHO - Marca: _____ Modelo: _____

Número de Série: _____ IMEI: _____

Acessórios: _____

Observação: _____

Data: ___/___/_____ Nome: _____

Registro: _____ Assinatura: _____

ANEXO III – TERMO DE DEVOLUÇÃO TELEFONE CELULAR CORPORATIVO

CHIP: ( ) Bom estado ( ) Com defeito

APARELHO: ( ) Bom estado ( ) Com defeito ( ) Faltando peças/acessórios

Observação: _____

Data: ___/___/____ Responsável pelo recebimento: _____

ANEXO IV – TERMO DE RECUSA TELEFONE CELULAR CORPORATIVO

Pelo presente recuso a utilização do celular/chip corporativo. Estou ciente que a Companhia me ofertou a possibilidade de aparelho/chip corporativo, entretanto opto em valer-se de meu próprio equipamento e linha telefônica. Estou de total acordo que, neste caso, o celular particular será utilizado também para fins laborais, cabendo a mim custeio de todas as despesas oriundas desse aparelho e linha telefônica, bem como manutenções e consertos.

Informo para os devidos fins que a linha que deixarei disponível para fins laborais, às minhas expensas será:

Núm. Linha: (13) _____

Observação: _____

Data: ___/___/_____ Nome: _____

Registro: _____ Assinatura: _____

Anuência do Sindicato

Data: ___/___/____

Assinatura: _____

ANEXO V – TERMO DE CIÊNCIA E RESPONSABILIDADE - USO DE DISPOSITIVOS PRÓPRIOS

Eu, _____, reg. _____, declaro ter ciência e responsabilidade dos seguintes tópicos em uso de equipamento pessoal para fins profissionais da Autoridade Portuária de Santos:

1. Possuo equipamento com sistema operacional e demais softwares licenciados.
2. Possuo equipamento com proteção ou nível de segurança equivalente ao adotado para os ativos da APS, ou seja, no mínimo um antivírus atualizado.
3. Possuo equipamento com os patches de segurança em dia.
4. É de uso exclusivo e não compartilhado com outras pessoas alheias à atividade laboral da APS.
5. É minha responsabilidade, a manutenção e a guarda deste equipamento, 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 devo comunicar imediatamente à GERID para que sejam adotadas as medidas cabíveis em relação à segurança e à privacidade das informações da APS.
6. Que ações de inspeção deste equipamento poderão ser conduzidas, e desde já autorizadas, implicando com isso, eventual acesso aos arquivos e dados pessoais ali constantes, como fotos, documentos etc.

Dados do equipamento:

- Marca: _____.
- Modelo: _____.
- Número de série: _____.

Por estar de acordo com as normas e procedimentos do Uso Aceitável de Ativos de TIC (disponível na Intranet) e suas atualizações, assumo total responsabilidade pelo presente termo.

Santos, ___ de _____ de _____

Assinatura: _____

Reg.: _____

ANEXO VI – TERMO DE RESPONSABILIDADE DE USO DE NOTEBOOK

Eu, _____, Reg. _____, declaro ter recebido, nesta data, da Gerência de Infraestrutura de Dados (GERID), os itens relacionados abaixo:

Item	Características	Patrimônio
1		
2		-

Declaro, também, ter ciência dos seguintes tópicos:

1. Conservar os ativos e seus acessórios em perfeitas condições de uso.
2. Utilizar para fins de trabalho, responsabilizando-me pelo uso indevido ou danos.
3. É proibida a instalação e utilização de softwares sem as devidas licenças de uso.
4. Solicitar mediante a chamado, instalação de softwares, drivers e periféricos, quando necessário.
5. Autorizo ações de auditoria de sistemas em equipamentos por mim utilizados, inclusive com total acesso aos dados pessoais ali constantes.
6. Comunicar imediatamente, via chamado, sobre qualquer incidente com os itens relacionados neste documento (incluindo, mas não se limitando a, perda, roubo, acesso não autorizado ou qualquer outra forma de comprometimento de dados).
7. Manter a confidencialidade e adotar medidas necessárias de proteção de todas as informações (especialmente dados pessoais), acessadas, processadas ou armazenadas no notebook, conforme a classificação de informação em vigor na APS.

Recomendações:

- Bloquear a tela do computador (teclas Windows+L), ao se ausentar do seu posto de trabalho.
- Evitar transportar o equipamento de forma visível (por exemplo, usar o porta-malas do carro).
- Não utilizar redes Wi-Fi de ambientes públicos, como: lan-houses.
- Procurar sempre prendê-lo com cadeado.
- Não permitir o uso por pessoas alheias ao trabalho.
- Cuidado com líquidos e outros resíduos.

Por estar de acordo com as normas e procedimentos de Entrega e Uso de Ativos de TI, assumo total responsabilidade pelo presente termo.

Santos, ___ de _____ de 2023

_____

Nome:_____

Reg. _____

INFORMAÇÕES DE CONTROLE

TÍTULO

MANUAL SGPI USO ACEITÁVEL DE ATIVOS DE TIC

VERSÃO

2.0

UNIDADE GESTORA DO DOCUMENTO

Superintendência de Tecnologia da Informação

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

- 5.9 INCLUÍDO PARA PREVER O USO DE FERRAMENTAS DE IA;
- 6 USUÁRIOS DO SERVIÇO DE E-MAIL CORPORATIVO, UNIFICA OS ITENS 6 E-MAIL CORPORATIVO E 7 USUÁRIOS DO SERVIÇO DE E-MAIL CORPORATIVO;
- 7.INFORMAÇÃO EM MÍDIA REMOVÍVEL, AJUSTA O ITEM 8. INFORMAÇÕES EM MÍDIA;
- 9.3 INCLUÍDO PARA DIFERENCIAR PROCEDIMENTOS RELATIVOS À APARELHOS CELULARES DA APS DOS DE PROPRIEDADE PARTICULAR;
- 10.2 INCLUÍDO VEDAÇÃO E CONDIÇÕES PARA ACESSO AOS RECURSOS DA APS UTILIZANDO DISPOSITIVOS PARTICULARES;
- 14.3 EXCLUÍDO;
- 16. APARELHOS CELULARES CORPORATIVOS, INCLUÍDO COM AJUSTES O NORMATIVO MANUAL PARA USO DE APARELHOS CELULARES DA AUTORIDADE PORTUÁRIA DE SANTOS S.A.
- RENUMERAÇÃO DOS ITENS CONSIDERANDO AS JUNÇÕES DE ITENS E OS NOVOS ITENS
- INCLUÍDOS OS ANEXOS DE I A VI.

RELAÇÃO COM OUTROS NORMATIVOS

Política de Segurança e Privacidade e SGPI;

Regulamento Interno de Pessoal da APS.

Código de Ética e de Conduta e Integridade;

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

NORMATIVOS REVOGADOS

MANUAL PARA USO DE APARELHOS CELULARES DA AUTORIDADE PORTUÁRIA DE SANTOS S.A.

INSTÂNCIA DE APROVAÇÃO

PRESIDENTE DA APS, POR MEIO DO PROCESSO VIRTUAL Nº 000099/22-91, EM 25/04/2024.