



**CARTILHA DE
UTILIZAÇÃO DE**

**RECURSOS
COMPUTACIONAIS**

INTRODUÇÃO

A Cartilha sobre Utilização de Recursos Computacionais da Santos Port Authority é um documento com recomendações, dicas que simplificam a aplicação das boas práticas que devem ser utilizadas pelos usuários de todos e quaisquer equipamentos relacionados à Tecnologia da Informação e Comunicação (TIC).

SUMÁRIO

1. O QUE É UM RECURSO COMPUTACIONAL?	3
2 - QUEM PODE REQUISITAR OS RECURSOS DA COMPANHIA?	4
3 - COMO SOLICITAR USUÁRIO DE REDE, ACESSO AO SAP, INTRANET E E-MAIL CORPORATIVO?	5
4 - COMO ACESSO AO SERVIDOR CENTRAL DE REDE E TRANSFERO MEUS DOCUMENTOS PARA ELE?	6
5 - COMO FAÇO PARA ACESSAR O PORTAL DA INTRANET DA SANTOS PORT AUTHORITY?	7
6 - CONSIGO ACESSAR A INTRANET FORA DA REDE DA SANTOS PORT AUTHORITY?	8
7 - CONSIGO ACESSAR O E-MAIL PELO SITE DO PORTO DE SANTOS?	9
8 - A QUE RISCOS UM COMPUTADOR VULNERÁVEL ESTÁ EXPOSTO?	12
9 - COMO POSSO PROTEGER O MEU COMPUTADOR?	13
10 - COMO POSSO RECUPERAR/ALTERAR MINHA SENHA DO WINDOWS, DA INTRANET, DO E-MAIL OU DO SAP?	15
11 - POSSO ACESSAR O SITE QUE DESEJAR?	16

1. O QUE É UM RECURSO COMPUTACIONAL?

É todo e qualquer componente virtual ou físico de disponibilidade limitada dentro de um ambiente computacional.

Pode ser um **computador, um e-mail, login de rede, e demais dispositivos**

integrantes da rede interna da empresa ou nela conectados.



ATENÇÃO

Os recursos computacionais da empresa devem ser utilizados de acordo com o disposto nesta cartilha. E por razões de padronização e segurança somente a área de TIC está habilitada a manusear, modificar e monitorar as configurações dos recursos computacionais e suas utilizações.

2 - QUEM PODE REQUISITAR OS RECURSOS DA COMPANHIA?

Todo funcionário, estagiário ou terceiro poderá utilizar os recursos da Companhia. Para isso, seu superior direto, ou gestor do contrato, quando terceiro, deve abrir um chamado no sistema de gestão de serviços, disponível na intranet.

3 - COMO SOLICITAR USUÁRIO DE REDE, ACESSO AO SAP, INTRANET E E-MAIL CORPORATIVO?

Para funcionários novos,

o RH já comunica a TIC para a criação dos usuários de rede, SAP, e-mail e intranet.

A própria Central de Serviços entra em contato para informar os dados de usuário e senha.

Para os demais funcionários

que ainda não contam com o recurso, basta abrir um chamado preferencialmente no sistema de gestão de serviços, disponível na intranet (Suporte ao Usuário).

4 - COMO ACESSO AO SERVIDOR CENTRAL DE ARQUIVOS E TRANSFIRO MEUS DOCUMENTOS PARA ELE?

O usuário ou o seu setor tem o direito de armazenar informações consideradas de importância ou de sigilo para a Companhia. Basta abrir um chamado preferencialmente no sistema de gestão de serviços, disponível na intranet (Suporte ao Usuário).

A partir dessa solicitação, a área de TIC entrará em contato com o requisitante que tomará as devidas providências para mapeamento da unidade de rede, criação e permissão do usuário à pasta reservada no servidor central.

Trata-se de um espaço reservado somente para armazenagem de arquivos corporativos.



ATENÇÃO

Qualquer arquivo que expressamente não pertença à Companhia ou que não esteja relacionado ao seu ambiente de trabalho será deletado sem prévia consulta.

5 - COMO FAÇO PARA ACESSAR O PORTAL DA INTRANET DA SANTOS PORT AUTHORITY?

A Intranet da Santos Port Authority poderá ser acessada pelo navegador no endereço

intranet.portodesantos.com.br
(10.0.10.3),

porém com restrições de acesso.

Para acessar todo o conteúdo da intranet permitido ao seu perfil, o usuário deve entrar no sistema com suas informações de login e senha.

6 - CONSIGO ACESSAR A INTRANET FORA DA REDE DA SANTOS PORT AUTHORITY?

Sim, seguindo os seguintes passos:

- 1) **Acesse o site**
<http://www.portodesantos.com.br>
- 2) Em “Área do Colaborador”, clique em “Intranet da Santos Port Authority”
- 3) Serão solicitados ao usuário seu login e senha de acesso



7 - CONSIGO ACESSAR O E-MAIL PELO SITE DO PORTO DE SANTOS?

Sim, seguindo os seguintes passos:

- 1) **Acesse o site**
<http://www.portodesantos.com.br>
- 2) Em “Área do Colaborador”, clique em “Webmail”
- 3) Serão solicitados ao usuário seu login e senha de acesso

É importante destacar que, por configurações padrões, e-mails baixados por meio do Outlook ficam armazenados na máquina, e geralmente não podem ser reabertos no webmail.

É aconselhável que o usuário periodicamente limpe seu e-mail, excluindo itens desnecessários, evitando assim que sua caixa de entrada fique cheia.



OBSERVAÇÃO

Caso o usuário não tenha acesso ao Sistema de Gestão de Serviço na Intranet, deve enviar um e-mail para: suporte.ti@portodesantos.com.br ou, em último caso, ligar no ramal 2020.

SEGURANÇA

A Santos Port Authority deve praticar esforços razoáveis e cumprir com os requisitos legais para garantir privacidade, confidencialidade, integridade e disponibilidade das informações geradas, processadas, armazenadas e transmitidas como parte integrante das suas atividades comerciais.

8 - A QUE RISCOS UM COMPUTADOR VULNERÁVEL ESTÁ EXPOSTO?



Captura de informações;



Uso do computador para atacar servidores e outros computadores;



Perda de dados;



Sequestro de dados (com pedido de resgate);



Sequestro de capacidade de processamento de dados para execução de tarefas de terceiros (ex.: mineração de criptomoedas);



Sequestro de identidade (uma pessoa se faz passar por outra em aplicativos de email e redes sociais);



Instalação de programas maliciosos ou com finalidades criminosas;



Acesso indevido a dados e informações;



Suspensão/Indisponibilidade dos serviços, sistemas e informações;

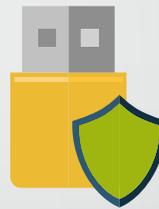


Uso do mesmo para práticas criminosas em outros computadores/servidores, visando qualquer um dos riscos acima ou combinação deles.

9 - COMO POSSO PROTEGER O MEU COMPUTADOR?

NUNCA desinstale os aplicativos “clientes” do antivírus e do software de inventário, o OCS. Caso estes softwares não estejam instalados no computador, o usuário, deve comunicar a Central de Serviços (SEOTI) imediatamente.

Não acesse, baixe ou instale programas não autorizados, pirateados ou suspeitos.



Tenha cuidado, existem sites com conteúdo impróprio ou ilegal que são porta de entrada para invasões.

Procure salvar seus documentos na rede, one drive ou sharepoint, estes ambientes são protegidos por cópia de segurança (backup). Dados locais (C:\) não são inclusos nos backups da SPA.

Evite trazer para a empresa mídias removíveis (CD, DVD, pen-drives ou quaisquer outros dispositivos móveis), mas caso seja necessário, respeite as boas práticas de utilização.

É proibida a gravação de dados sigilosos, que desrespeitem a ética ou a legislação, e programas, sistemas e/ou softwares de propriedade da SPA em mídias removíveis.



Tome cuidado ao receber e-mails suspeitos com links e/ou anexos, mesmo para remetentes conhecidos. Muitas vezes esses endereços ou arquivos, aparentemente inofensivos, possuem alguma ameaça oculta, a qual é ativada quando aberta. Desconfie caso o assunto não faça sentido ou o e-mail solicite ações fora do comum.

Nunca forneça dados pessoais, principalmente bancários, por e-mail.

Não repasse ou divulgue seu login e senha mesmo para colegas de sessão.

Crie regularmente senhas complexas contendo caracteres alfa numéricos e especiais (@#!?_*). Uma senha não segura pode aumentar a vulnerabilidade do computador.



Não deixe informações sensíveis aparentes ou com fácil acesso público, como em anotações de cadernos ou post-its.

Ao se afastar do seu computador, bloqueie-o, sempre (teclas Windows + L).

10 - COMO POSSO RECUPERAR/ALTERAR MINHA SENHA DO WINDOWS, DA INTRANET, DO E-MAIL OU DO SAP?

A TIC não guarda as senhas de nenhum usuário e, em caso de perda/esquecimento, uma nova será atribuída. Basta abrir um chamado no sistema de gestão de serviços, disponível na intranet.

11 - POSSO ACESSAR O SITE QUE DESEJAR?

Sim, desde que ele tenha relação direta com sua rotina de trabalho.



ATENÇÃO

O acesso aos sites não permitidos pode gerar sanções ao funcionário, dependendo da gravidade da ação.

Caso algum site seja essencial à função desempenhada esteja bloqueado, o usuário deverá solicitar seu desbloqueio, declarando o site desejado e o motivo do acesso, com a abertura de chamado no sistema de gestão de serviços, disponível na intranet. Este processo é executado pela Central de Serviços, que solicitará ao seu gestor um e-mail com a aprovação da requisição e encaminhará à área responsável.

Alguns sites são bloqueados pelos próprios mecanismos de segurança presentes na companhia ao se detectar algum comportamento ou recurso suspeito ou conhecidamente malicioso no site acessado.

