<table>
<tr><td rowspan="5">SANTOS PORT AUTHORITY</td><td colspan="4">SANTOS PORT AUTHORITY</td></tr>
<tr><td colspan="3">Instrumento Normativo de Processo</td><td>Código: TIC.140-009</td></tr>
<tr><td>Diretoria Responsável:
Presidência</td><td colspan="2">Unidade Responsável:
Superintendência de Tecnologia da Informação</td><td>Elaboração:
Supervisão de Governança de TI</td></tr>
<tr><td>Início da vigência:
05/08/2021</td><td>Próxima revisão:
05/08/2023</td><td>Aprovação:
Decisão Direxe nº
316.2021</td><td>Validação:
Superintendente de Tecnologia da Informação</td></tr>
<tr><td colspan="3">Processo: Sistema de Gestão da Privacidade da Informação: Gestão de Acessos</td><td>Versão: 1.2</td></tr>
</table>

Instrumento Normativo de Processo

Sistema de Gestão da Privacidade da Informação: Gestão de Acessos

SUMÁRIO

1. OBJETIVO **3**

2. ABRANGÊNCIA **3**

3. FUNDAMENTAÇÃO **3**

4. DEFINIÇÕES **3**

5. ARCABOUÇO LEGAL **5**

6. DIRETRIZES **5**

6.1. Diretrizes ***5***

6.2. Consenso / Aprovação ***7***

7. PAPÉIS E RESPONSABILIDADES **7**

7.1. Da Unidade Responsável ***7***

7.2. Das Unidades Executoras ***7***

8. DISPOSIÇÕES FINAIS **8**

9. ANEXOS **8**

1. OBJETIVO

Definir as atividades para o gerenciamento de direitos de acesso de usuários aos sistemas corporativos e à Intranet da SPA, bem como suas respectivas responsabilidades.

2. ABRANGÊNCIA

Todos os sistemas corporativos que são utilizados em ambientes de produção na *Santos Port Authority* – SPA, e se aplica a todos os funcionários, os cedidos, os estagiários e os terceirizados que executem atividades nas instalações da Companhia.

3. FUNDAMENTAÇÃO

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

4. DEFINIÇÕES

Termo	Descrição
Conta de Serviço	Contas utilizadas para acessos automáticos à sistemas. Ex: Login para conexão com o Banco de Dados.
Gestor Responsável	Pessoas que normalmente respondem por um setor na SPA, como Superintendente, Gerente ou Supervisor
***Login* genérico**	Contas genéricas que são compartilhadas entre usuários. Ex: estagiario.supti@brssz.com.
Logon	Ação de realizar acesso ao sistema de informação.
Perfis de Acesso	Funções pré-determinadas que correspondem aos direitos e permissões dados a um grupo específico de usuários.
Segregação de Funções	Consiste na separação de funções, nomeadamente de autorização, aprovação, execução, controle e contabilização das operações.
Senha provisória	Senha destinada para realizar o primeiro acesso do usuário ao sistema, sendo substituída logo em seguida à criação de uma nova senha pelo usuário no primeiro *logon*.
Sistema de Chamados	Sistema específico da TI, de responsabilidade da Gerência de Operação e Soluções de TIC, disponibilizado na Intranet da SPA para a abertura de chamados técnicos relacionados aos ativos de Tecnologia da Informação.

Termo	Descrição
Utilitários de sistema operacional	Aplicativos disponibilizados pelo Sistema Operacional para a administração dos recursos tecnológicos do ativo físico utilizado.
Matriz de Segregação de Funções	Refere-se a práticas nas quais o conhecimento e/ou privilégios necessários para se completar um processo são quebrados e divididos entre múltiplos usuários de forma que apenas um seja capaz de executá-lo ou controlá-lo sozinho. A principal razão de se aplicar a segregação de funções é prevenir a realização e ocultação de fraude e erro no curso normal das atividades, uma vez que havendo mais de uma pessoa para realizar uma atividade se minimiza a oportunidade de transgressões e aumenta as chances de se detectá-la, assim como de se detectar erros não intencionais. Considera-se as Responsabilidades, detecção de conflitos na realização de tarefas e alçadas e constante revisão.
Gestão de Usuários e Senhas	Conjunto de atividades relacionadas aos acessos pelos usuários: • Criação de identidade • Identificação • Senhas provisórias • Gestão de Senhas • Usuário Administrador ○ Especificação • Restrições
Contas de Serviço	Trata-se de contas utilizadas na execução de atividades automatizadas em computadores.
Acessos Temporários	Acessos fornecidos para execução de atividades por terceiros, estagiários, menores aprendiz, contratado ou quem se assemelhe, com tempo determinado.
Análise crítica	Atividade periódica de análise dos privilégios dados aos usuários para acesso aos ativos de TI, considerando: • Documentação • Histórico • Escopo

Termo	Descrição
Controle de Acesso a Sistemas e Aplicações.	Conjunto de atividades de controle visando o acesso a Sistemas e Aplicações. Considera-se: • Restrição de acesso à Informação; • Procedimentos seguros de inicialização (*logon*); • Uso de programas utilitários privilegiados; • Controle de acesso para código fonte.

5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
Resolução CGPAR nº 11 de 10/05/2016	2016	Dispõe sobre o planejamento e implementação de práticas de governança de Tecnologia da Informação (TI) que atendam de forma adequada os padrões usualmente reconhecidos nesta área, pelas empresas estatais federais.
ISO/IEC 27001:2013	2013	*Information technology --Security techniques -Information security management systems --Requirements*
ISO/IEC 27002:2013	2013	*Information technology --Security techniques --Code of practice for information security controls* (Tecnologia da Informação – Técnicas de Segurança –Código de práticas para controles de segurança da Informação)
ISO/IEC 27005:2010	2010	*Information technology --Security techniques -Information security risk management* (Tecnologia da Informação – Técnicas de Segurança –Gerenciamento Riscos Segurança Informação)
ISO/IEC 27701:2019	2019	*Information technology --Security techniques -Privacy Information Management System (PIMS)* (Tecnologia da Informação –Técnicas de Segurança –Sistema de Gestao da Privacidadeda Informação –SGPI)

6. DIRETRIZES

6.1. Diretrizes

#	ATIVIDADES
1	A Superintendência de Tecnologia da Informação (SUPTI) deve garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação da SPA.
Gestão de Acesso Lógico:	
2	A SUPTI deve limitar o acesso à informação e aos ativos de informação e recursos de processamento ao mínimo que permita o correto desempenho das atividades do cargo, função ou atribuições de cada usuário.
3	A credencial de acesso é pessoal e intransferível, permitindo de maneira clara e inequívoca o reconhecimento do usuário.
4	A senha do usuário deve: • ser pessoal e intransferível; • jamais ser genérica; • conter no mínimo 8 (oito) caracteres; • não ser atualizada com as 6 (seis) últimas senhas registradas; • estar invisível para qualquer pessoa; • conter no mínimo uma letra maiúscula e um caractere especial; • não pode conter números ou letras em sequência e nem nome próprio; • trocada a intervalos regulares.
5	A SUPTI deve utilizar ferramentas e/ou protocolos de proteção contra acessos não autorizados aos ativos de informação.
6	O usuário é responsável por todas as ações realizadas por meio de sua credencial de acesso.
7	A SUPTI deve revisar o acesso concedido a usuários, mediante informação da Superintendência de Gestão de Pessoas (SUGEP) e Saúde Ocupacional, que tiveram mudanças em suas atribuições, devendo ser readequados imediatamente ou bloqueados em caso de perda do vínculo com a Companhia.
8	A SUPTI em conjunto com a SUGEP, quando necessário, promoverá ações para a educação, treinamento visando a conscientização de todos os empregados sobre a aplicação das melhores práticas integradas para apoiar o processo de gestão de acesso.

#	ATIVIDADES
9	Compete aos concedentes de acesso e aos usuários, a observância das regras de uso, concessão e supressão de acessos estabelecidas em procedimentos, garantindo a segurança de seus usuários e a integridade da Companhia.
10	O usuário comunicará, com a brevidade adequada, a perda ou a desnecessidade de acesso, temporário ou finalístico, bem como comunicará atualizações relacionadas com seu nível de acesso, notadamente quando estes acarretarem a diminuição ou cessão de direitos.
11	Os direitos de acesso de todos os empregados às informações e aos recursos de processamento da informação devem ser retirados, pela SUPTI, mediante informação da Área de Recursos Humanos, imediatamente após o encerramento de suas atividades, contratos ou acordos.

6.2. Consenso / Aprovação

Este Instrumento Normativo deve ser aprovado pela Diretoria Executiva.

7. PAPÉIS E RESPONSABILIDADES

7.1. Da Unidade Responsável

Área	Atividades	Ferramenta
SUPTI	Responsável por apoiar a proteção da informação de todas as Unidades de Gestão dentro da SPA, através de controles tecnológicos, nos aspectos de sua: ○ identificação; ○ apresentação; ○ sustentação; ○ escolha; ○ implantação; e ○ manutenção.	N/A

7.2. Das Unidades Executoras

Área	Atividades	Ferramenta
SUPTI	Responsável por: ○ assegurar o gerenciamento adequado dos perfis de acessos da Companhia, em conformidade a este normativo. ○ garantir: ○ o tratamento do controle de acesso dos usuários; ○ que não existam *logins* genéricos sem a prévia autorização da Superintendência de Tecnologia da Informação. ○ a individualidade dos *logins* (que um usuário não possua dois *logins* com o mesmo perfil em um sistema). ○ que todos os descansos de tela de computadores possuam senha para desbloqueio do computador. ○ verificar a utilização de *logins* através de logs de acesso.	N/A
SUGEP	Responsável por comunicar a Gerência de Infraestrutura de Dados (GERID) das: ○ admissões; ○ movimentações internas e externas; e ○ desligamentos de empregados, estagiários da Companhia.	E-mail

8. DISPOSIÇÕES FINAIS

Os casos omissos ou excepcionais neste Instrumento Normativo serão submetidos à análise e aprovação da Diretoria Executiva.

A não observância aos dispositivos desse documento pode acarretar, nos termos da legislação e normativos internos aplicáveis, sanções administrativas, civis e/ou penais.

9. ANEXOS

N/A