<table>
<tr><td rowspan="4"></td><td colspan="4">SANTOS PORT AUTHORITY</td></tr>
<tr><td colspan="3">Instrumento Normativo de Processo</td><td>Código: TIC-140-017</td></tr>
<tr><td colspan="2">Diretoria Responsável:
Presidência</td><td>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
317.2021</td><td>Validação:
Superintendente de Tecnologia da Informação</td></tr>
<tr><td colspan="3">Processo: Sistema de Gestão da Privacidade da Informação: Segurança da Informação na gestão da continuidade de negócio.</td><td>Versão: 1.1</td></tr>
</table>

Instrumento Normativo de Processo Sistema de Gestão da Privacidade da Informação: Gestão de Continuidade de Negócio

SUMÁRIO

1. OBJETIVO

Estabelecer que as diretrizes da continuidade da segurança da informação sejam contempladas nos sistemas de gestão da continuidade do negócio da organização.

2. ABRANGÊNCIA

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

3. FUNDAMENTAÇÃO

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

4. DEFINIÇÕES

Termo	Descrição
PCN	Plano de Continuidade de Negócios

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	Continuidade da segurança da informação: Determinar por meio da Superintendência de Tecnologia da Informação (SUPTI) os requisitos para a segurança da informação e a continuidade da gestão da segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre. Avaliar se a continuidade da segurança da informação está contida dentro do processo de gestão da continuidade do negócio ou no processo de gestão de recuperação de desastre.
IMPLEMENTAÇÃO DA CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO	
2	Estabelecer, documentar, implementar e manter processos, procedimentos e controles, através da SUPTI, para assegurar o nível requerido de continuidade para a segurança da informação, durante uma situação adversa. Considerar: ○ Implementar uma estrutura de gerenciamento para mitigar e responder a um evento de interrupção, com pessoas com experiência, competência e a necessária autoridade; ○ Aprovar, junto à Diretoria Executiva, planos documentados, procedimentos de recuperação e resposta, detalhando como a SPA irá gerenciar um evento de interrupção de negócios e como a segurança da informação será mantida num nível que atenda aos objetivos predeterminados de continuidade da segurança da informação.
3	Estabelecer, documentar, implementar e manter, através da SUPTI: ○ Controles de segurança da informação dentro dos processos de recuperação de desastres ou continuidade do negócio, incluindo procedimentos, ferramentas e sistemas de suporte; ○ Processos, procedimentos e mudanças de implementação para manter os controles de segurança da informação existentes durante uma situação adversa; ○ Controles compensatórios para os controles de segurança da informação que não possam ser mantidos durante uma situação adversa.

#	ATIVIDADES
4	Verificação, análise crítica e avaliação da continuidade da segurança da informação: • Testar e verificar a funcionalidade dos processos, procedimentos e controles da continuidade da segurança da informação para garantir que eles sejam consistentes com os objetivos da continuidade da segurança da informação; • Testar e verificar o conhecimento e a rotina para operar os procedimentos, processos e controles de continuidade da segurança da informação, de modo a assegurar que o seu desempenho esteja consistente com os objetivos da continuidade da segurança da informação; • Proceder análise crítica quanto à validade e eficácia dos controles de continuidade da segurança da informação, quanto aos sistemas de informação, processos de segurança da informação, procedimentos e controles ou gestão da continuidade do negócio/gestão de recuperação de desastre e soluções de mudança.
5	Redundâncias: Assegurar a disponibilidade dos recursos de processamento da informação.
6	Disponibilidade dos recursos de processamento da informação, através da SUPTI: Assegurar que os recursos de processamento da informação sejam implementados com redundância suficiente para atender aos requisitos de disponibilidade.

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	Aplicação das políticas, práticas, instrumentos normativos e POPs de Segurança da Informação. Responsável pelos controles tecnológicos que apoiam a proteção da informação de todas as Unidades de Gestão da SPA, nos aspectos de: • Identificação; • apresentação; • sustentação; • escolha; • implantação; e, • manutenção.	N/A

8. DISPOSIÇÕES FINAIS

Os casos omissos ou excepcionais neste Instrumento Normativo deverão ser 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.