

	SANTOS PORT AUTHORITY		
	Instrumento Normativo de Processo		Código: TIC-140-012
	Diretoria Responsável: Presidência	Unidade Responsável: Superintendência de Tecnologia da Informação	Elaboração: Supervisão de Governança de TI
	Início da vigência: 28/10/2021	Próxima revisão: 28/10/2023	Aprovação: Decisão Direxe nº 450.2021
Processo: Sistema de Gestão da Privacidade da Informação: Segurança nas Operações			Versão: 1.2

Instrumento Normativo de Processo

Sistema de Gestão da Privacidade da Informação: Segurança nas Operações

SUMÁRIO

1. OBJETIVO	3
2. ABRANGÊNCIA.....	3
3. FUNDAMENTAÇÃO	3
4. DEFINIÇÕES	3
5. ARCABOUÇO LEGAL	6
6. DIRETRIZES	7
6.1. Diretrizes	7
6.2. Consenso / Aprovação	15
7. PAPÉIS E RESPONSABILIDADES.....	15
7.1. Da Unidade Responsável.....	15
7.2. Das Unidades Executoras	16
8. DISPOSIÇÕES FINAIS	16
9. ANEXOS.....	16

1. OBJETIVO

Estabelecer as diretrizes a serem adotadas no processo de Segurança nas Operações com vistas a garantir a operação segura e correta dos recursos de processamento da informação.

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
Acesso de Administradores	Acesso efetuado à ativos de TI com direitos de Administração sobre o ativo. Direito de administrador tem total poder sobre o funcionamento do ativo de TI.
EC-Council	Conselho Internacional de Consultores de Comércio Eletrônico. É uma organização americana que oferece certificação, educação, treinamento e serviços em segurança cibernética em várias habilidades de segurança cibernética. <small>Fonte: Wikipedia</small>
Hotfix	Pacote cumulativo que inclui um ou mais arquivos que são usados para endereçar um problema num produto de <i>software</i> (isto é, uma parte de <i>software</i>). São feitos para endereçar uma situação específica. Um <i>hotfix</i> , ou mesmo um conjunto de <i>hotfixes</i> , pode ser um pacote usado para corrigir uma série de <i>bugs</i> (falhas), seja em aplicativos ou no próprio sistema. Um exemplo bem tangível são as atualizações de segurança, que objetivam sanar as vulnerabilidades.
Gestão de Vulnerabilidades	Processo contínuo de identificação, avaliação e eliminação de vulnerabilidades, por meio da realização de testes de vulnerabilidade.

Termo	Descrição
<p align="center">Código de ética da EC-Council</p>	<p>Código de ética utilizada como parâmetro por profissionais especializados na atividade de “hackeamento” ético.</p> <p>Fonte: https://www.eccouncil.org/code-of-ethics/ (tradução em https://www.diegomacedo.com.br/hacker-etico/).</p> <ol style="list-style-type: none"> i. Manter a confidencialidade das informações obtidas durante os testes, não podendo vender ou repassar sem a permissão por escrito do cliente; ii. Proteger a propriedade intelectual dos outros; iii. Divulgar às pessoas apropriadas ou autoridades, os perigos de qualquer cliente de e-commerce, da comunidade da internet ou de qualquer pessoa relacionada a uma transação eletrônica via software ou hardware; iv. Prover um serviço com qualidade dentro da sua área de conhecimento e sendo honesto quanto a sua capacidade técnica; v. Nunca usar um software obtido de forma ilegal ou antiética; vi. Não se envolver em práticas financeiras fraudulentas como suborno, dupla cobrança ou práticas financeiras inadequadas; vii. Usar as informações do cliente ou empregador de forma consciente e somente o que foi autorizado; viii. Ter uma conduta de forma ética e competente o tempo inteiro; ix. Não ter envolvimento com hackers ou atividades maliciosas; x. Não comprometer de forma proposital os sistemas dos clientes durante sua atividade profissional; xi. Garantir que todos os pentests sejam autorizados e dentro da legalidade; xii. Não violar nenhuma lei.

Termo	Descrição
<p>“Hacking” ilegal</p>	<p>É um crime sujeito a punição nos termos de leis internacionais e nacionais. Nos EUA, a lei de <i>hacker</i> assinada por Barak Obama, pode tornar uma pessoa, inconscientemente, um criminoso” (thenextweb.com January 2015)</p> <p>Legislações internacionais (algumas)</p> <ul style="list-style-type: none"> • Europa: 2002 Diretiva ePrivacy • Europa: 2013 Uma Diretiva sobre ataques contra sistemas de informação. Fonte Web: http://db.euocrim.org/db/en/vorgang/252/ • EUA Leis Federais sobre Cybercrime (comportamentos ilícitos) <ul style="list-style-type: none"> ○ Fraude na Internet; ○ Pirataria de Software (Roubo de Propriedade Intelectual). • Brasil: Lei que tipifica crimes cibernéticos ou informáticos: Lei 12.737/12: <ul style="list-style-type: none"> ○ Invadir dispositivos alheios; ○ Obter, adulterar ou destruir criminalmente dados; ○ Instalar vulnerabilidade em dispositivos; ○ Produzir, oferecer, distribuir, vender ou difundir meios para invasão de dados.
<p>Hacking ético</p>	<p>Atividade executada por qualquer indivíduo que é treinado para dominar tecnologias de “hacking” (burlar a segurança de um sistema computacional, buscando acessar ilegalmente, sem a permissão do dono, um computador ou sistema computacional e informático.</p> <p>Fonte: https://www.dicio.com.br/hackeado/</p>
<p>Malware</p>	<p>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 <i>software</i> hostil ou intruso.</p>

Termo	Descrição
Patches	Um tipo de <i>hotfix</i> que corrige algo que, por algum motivo, não está funcionando do jeito que deveria dentro de um determinado <i>software</i> . Os <i>patches</i> mais comuns são conhecidos como <i>bugfix</i> . Esses são criados e implementados para remediar erros e <i>bugs</i> que se fazem presentes no sistema. Os <i>patches</i> mais comuns têm a ver com vulnerabilidades de segurança. Ou seja, se algum <i>software</i> apresentou uma falha que possa fazer com que dados importantes sejam vazados ou explorados por criminosos, o <i>patch</i> atua nessa correção.
Teste de Vulnerabilidade	Teste ou avaliação de segurança, sem intenção maliciosa ou criminosa, compondo um dos pilares do esforço para tornar a rede corporativa da SPA mais segura (<i>hacking</i> ético) e identificar vulnerabilidades.

5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
Decreto nº 9.637	2018	Institui a Política Nacional de Segurança da Informação.
Resolução CGPAR nº 11	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	<i>Information technology --Security techniques - Information security management systems -- Requirements</i>
ISO/IEC 27002:2013	2013	<i>Information technology --Security techniques --Code of practice for information security controls</i> (Tecnologia da Informação –Técnicas de Segurança –Código de práticas para controles de segurança da Informação)
ISO/IEC 27005:2010	2010	<i>Information technology --Security techniques - Information security risk management</i> (Tecnologia da Informação –Técnicas de Segurança – Gerenciamento Riscos Segurança Informação)
ISO/IEC 27701:2019	2019	<i>Information technology --Security techniques - Privacy Information Management System (PIMS)</i> (Tecnologia da Informação –Técnicas de Segurança –Sistema de Gestao da Privacidade da Informação – SGPI)

6. DIRETRIZES

6.1. Diretrizes

#	Diretrizes
1	<p>A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) dos procedimentos de operação de TI para:</p> <ul style="list-style-type: none"> ○ Instalação e configuração de Sistemas; ○ Tratamento da informação: processamento automático ou manual; ○ Cópias de Segurança; ○ Tratamento de erros que possam ocorrer durante a execução de uma tarefa; ○ Contatos para suporte e escalção; ○ Manuseio de mídias, formulários especiais, dados confidenciais, descarte seguro e resultados provenientes de falhas de operação; ○ Reinício e recuperação de sistemas; ○ Gestão de trilhas de auditoria e registros (<i>logs</i>) de sistemas; ○ Monitoramento.
GESTÃO DE MUDANÇAS	
2	<p>A SUPTI deve definir controles para os seguintes itens:</p> <ul style="list-style-type: none"> ○ Identificação e registro de mudanças significativas; ○ Planejamento e testes de mudanças; ○ Avaliação de impactos de segurança da informação de tais mudanças; ○ Procedimentos de aprovação de mudanças propostas; ○ Verificação de que os requisitos de segurança da informação foram atendidos para as mudanças; ○ Comunicação das mudanças para todas as pessoas relevantes; ○ Procedimentos de recuperação e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados; ○ Provisão de um processo emergencial de mudança que permita a implementação rápida e controlada de mudanças, necessárias para resolver um incidente.
GESTÃO DA CAPACIDADE	

#	Diretrizes
3	<p>A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) referentes a:</p> <ul style="list-style-type: none"> ○ Exclusão de dados obsoletos (espaço em disco); ○ Desativação de aplicações, sistemas, base de dados e ambientes fora de uso; ○ Otimização de processamento em lote; ○ Otimização da lógica para aplicações ou consultas à base de dados; ○ Gerenciamento da largura de banda para serviços que demandam recursos.
SEPARAÇÃO DOS AMBIENTES DE DESENVOLVIMENTO, TESTE E PRODUÇÃO	
4	<p>A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) referentes a:</p> <ul style="list-style-type: none"> ○ Regras para transferência de código do ambiente de desenvolvimento para o de produção; ○ Executar <i>software</i> de desenvolvimento e <i>software</i> de produção em diferentes sistemas ou processadores ou domínios ou partições sempre que possível; ○ Testar mudanças nas aplicações em ambiente de testes antes de serem aplicadas; ○ Não realizar testes em sistemas operacionais; ○ Compiladores, editores, ferramentas de desenvolvimento e utilitários de sistemas não sejam acessíveis aos sistemas operacionais; ○ Perfis diferentes para usuários de teste e de produção, com mensagens apropriadas para identificação e redução de erros; ○ Dados sensíveis ou pessoais não podem ser copiados para ambientes de testes sem controles equivalentes de segurança da informação.
PROTEÇÃO CONTRA MALWARE	
5	É proibido o uso de qualquer aplicação, utilitário ou <i>software</i> não autorizado.

#	Diretrizes
6	<p>A SUPTI deve definir e monitorar:</p> <ul style="list-style-type: none"> ○ Controles para detectar o uso de <i>software</i> não autorizado em execução; ○ Controles para detectar acesso a sítios maliciosos, suspeitos, ou de uso contrário às recomendações da SPA; ○ Procedimentos Operacionais Padrão (POP) para reduzir vulnerabilidades exploradas por <i>malware</i> através de rotinas de gerenciamento de vulnerabilidades técnicas; ○ Procedimentos e as responsabilidades no tratamento da proteção contra <i>malware</i>; ○ Planos de Continuidade de Negócios para recuperação em caso de ataques por <i>malware</i>, incluindo cópia de segurança dos dados e sistemas; isolar os ambientes onde impactos negativos possam ocorrer.
7	<p>A SUPTI deve executar análises críticas regulares em <i>softwares</i> e dados de sistemas que suportam processos classificados críticos para o negócio, bem como investigar formalmente a presença de qualquer arquivo não aprovado para uso.</p>
8	<p>A SUPTI deve instalar e manter <i>software</i> para detecção e remoção de <i>malware</i> em servidores e estações de trabalho incluindo:</p> <ul style="list-style-type: none"> ○ Varredura em arquivos recebidos; ○ Varredura em e-mail recebidos; ○ Varredura em páginas web.
CÓPIAS DE SEGURANÇA	
9	<p>A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) de cópias e restauração de dados, considerando:</p> <ul style="list-style-type: none"> ○ Armazenar as cópias de segurança em locais remotos, a uma distância considerada suficiente para escapar de danos resultantes de um desastre ocorrido no local principal; ○ Proteger física e ambientalmente o local onde as cópias de segurança estão armazenadas, consistentes com as mesmas proteções aplicadas no local principal; ○ Testar regularmente as médias de cópias de segurança, combinado com um teste de restauração; ○ Criptografar as cópias de segurança que contenham dados classificados como sigilosos.

#	Diretrizes
10	<p>Considera-se itens objeto de cópias de segurança:</p> <ul style="list-style-type: none"> ○ Códigos fontes de sistemas incluindo versionamentos; ○ Bancos de dados (SGBDs e outros arquivos de dados); ○ <i>Scripts</i>; ○ Caixas postais de e-mails e anexos; ○ Sistemas operacionais e utilitários diversos; ○ Servidores, principalmente os virtuais; ○ Configurações diversas de equipamentos; ○ Arquivos gerenciados pelo Office 365; ○ Fotos, vídeos e áudios relacionados às atividades da SPA; ○ Outros arquivos relacionados às atividades da SPA.
REGISTROS E MONITORAMENTO	
11	<p>A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP), bem como manter registros e monitoramento referentes a:</p> <ul style="list-style-type: none"> ○ Identificação de usuários (ID); ○ Atividades em sistemas; ○ Datas, horários e detalhes de eventos (<i>logon e logout</i>); ○ Identidade do dispositivo acessado e localização (quando possível); ○ Tentativas de acesso ao sistema (aceitas e rejeitadas); ○ Tentativas de acesso a outros recursos e dados (aceitas e rejeitadas); ○ Alterações de configurações do sistema; ○ Uso e atribuição de privilégios; ○ Uso de aplicações e utilitários de sistema; ○ Arquivos acessados e tipo de acesso; ○ Endereços e protocolos de rede; ○ Ativação de desativação dos sistemas de proteção (antivírus, etc); ○ Registros de transações executadas pelos usuários nas aplicações; ○ Proteger de forma adequada com controles de acesso e cópias de segurança todos os registros produzidos.
12	<p>A SUPTI deve utilizar uma única fonte de tempo – íntegra – para sincronizar a hora/data de todos os sistemas de processamento de informações, dentro da SPA ou de seu domínio de segurança.</p>
INSTALAÇÃO DE SOFTWARE EM SISTEMAS OPERACIONAIS	
13	<p>Somente usuários com direitos e acesso de administradores podem atualizar sistemas operacionais, aplicativos e bibliotecas de programas.</p>
14	<p>Sistemas operacionais e de aplicativos só podem ser implementados após testes bem-sucedidos.</p>

#	Diretrizes
15	A SUPTI deve manter documentação dos controles sobre a implementação e configuração de sistemas operacionais, bem como implementação de bibliotecas de programas.
16	A SUPTI deve manter estratégia de retorno às condições anteriores antes que mudanças sejam implementadas em sistemas operacionais e bibliotecas de programas.
17	A SUPTI deve manter registro de auditoria para todas as atualizações das bibliotecas de sistemas e programas.
18	A SUPTI deve manter versões anteriores de <i>software</i> aplicativos como medida de contingência.
GESTÃO DE VULNERABILIDADES TÉCNICAS	
19	A SUPTI deve definir e estabelecer funções e responsabilidades associadas à gestão de vulnerabilidades técnicas, incluindo as atividades de monitoramento, avaliação de riscos, correções, acompanhamento e necessidades de escalação em caso de ocorrência de incidentes.
20	A SUPTI deve avaliar os riscos associados e criar Planos de Ação para mitigar estes riscos para cada vulnerabilidade técnica potencial identificada pela área de riscos e controles internos em conjunto com a SUPTI.
21	A SUPTI deve avaliar os riscos associados à instalação de correções (<i>patches</i> e <i>hotfix</i>) disponibilizados.
22	<p>A SUPTI deve testar e avaliar as correções disponibilizadas pela TI assegurando sua efetividade. Em caso de não existir a disponibilidade de uma correção, considerar medidas compensatórias:</p> <ul style="list-style-type: none"> ○ Desativar os serviços relacionados à vulnerabilidade; ○ Adaptar ou agregar controles de acesso; ○ Aumentar a frequência de monitoramento para prevenir ou detectar um ataque real; ○ Aumentar a conscientização sobre a vulnerabilidade.
23	A SUPTI deve manter registro de auditoria de todos os procedimentos realizados, bem como avaliar e monitorar regularmente o processo de gestão de vulnerabilidades.
24	A SUPTI deve priorizar os sistemas críticos de negócio.

#	Diretrizes
25	A SUPTI deve alinhar a gestão de vulnerabilidades com a gestão de incidentes, comunicando os dados sobre vulnerabilidades às funções de respostas a incidentes juntamente com Procedimentos Operacionais Padrão caso ocorra um incidente.
26	<p>A Gerência de Infraestrutura de Dados (Gerid) deve efetuar teste de vulnerabilidade periodicamente a cada 6 meses e em caso de:</p> <ul style="list-style-type: none"> a. Mudanças na infraestrutura de ti; b. Novos serviços implantados; c. Alterações nos serviços existentes; <p>Eliminação de vulnerabilidades (verificação de eficácia de medidas de eliminação).</p>
27	<p>Ativos de TI da SPA, que podem ser objeto de varredura para identificação de vulnerabilidades:</p> <ul style="list-style-type: none"> a. Servidores de autenticação; b. Servidores de arquivos; c. Servidores de aplicação; d. Servidores DNS; e. Servidores DHCP; f. Servidores WEB e FTP; g. Servidores de e-mail; h. Servidores de banco de dados; i. Outros servidores que hospedem outros serviços (ex VPN, etc); j. Sistemas Gerenciadores de Banco de Dados (SGBD) e Bancos e/ou instancias gerenciados por cada um dos SGBD; k. Equipamentos ativos de rede com gerenciamento (<i>switches, gateways, firewalls, roteadores</i>); l. Sistemas <i>Web-based</i>; m. Outros ativos de TI, pertencentes à SPA e que estejam no ambiente da SPA. <p>Ativos não pertencentes à SPA, mas que estejam no ambiente da SPA, devem ser testados em comum acordo com o proprietário e sua participação no planejamento, execução se pertinente, e conclusão;</p> <p>Obs.: Ativos de Ti hospedados em nuvem, ou hospedados por terceiros, não devem ser testados por poder caracterizar atividade ilegal (“hackeamento” ilegal). Nesse caso, solicitar evidência quanto a segurança do ambiente.</p>
28	É proibida a utilização das ferramentas e técnicas de detecção de vulnerabilidades com o objetivo de – ilegalmente - invadir e/ou obter qualquer informação de qualquer ativo de Ti da SPA ou de terceiros.

29	<p>Ferramentas e técnicas devem ser utilizadas para:</p> <ol style="list-style-type: none">a. Detecção de rede (<i>sniffing</i>), cabeada e sem fio;b. Varredura para identificação de vulnerabilidades nos ativos de TI; <p>Lista (não exaustiva) de vulnerabilidade a serem testadas:</p> <ol style="list-style-type: none">a. Vulnerabilidades em sistemas <i>Web-based</i> (exemplos)<ol style="list-style-type: none">i. Injeção de SQL;ii. Scripts cruzados (cliente e servidor);iii. Inclusão de arquivos remotos;iv. Sequestro de sessão;b. Vulnerabilidades em bancos de dados (exemplos):<ol style="list-style-type: none">i. Nomes de tabelas de autenticação;ii. Acesso a senhas;c. Vulnerabilidades em redes sem fio (exemplos):<ol style="list-style-type: none">i. Chaves de acesso (WEP/WPA);ii. Senhas fracas;d. Vulnerabilidades em servidores (exemplos):<ol style="list-style-type: none">i. Inclusão remota de arquivos;ii. <i>Bind e Back Shells</i>; <p>O planejamento do teste deve considerar:</p> <ol style="list-style-type: none">a. Indicação do ativo ou ativos a serem testados (candidato a vulnerabilidade);b. Indicação do tipo de teste:<ol style="list-style-type: none">i. Teste caixa preta: Não necessita nenhum conhecimento de estruturas internas ou funcionamento.ii. Teste caixa branca: Necessita de conhecimento completo de estruturas internas e funcionamento.iii. Teste caixa cinza: Necessita de conhecimento relevante apenas para os testes específicos.c. Indicação do ambiente para o teste, inclusive se será feito a partir do ambiente interno e/ou externo, em cópia do ativo de TI para esse fim ou o ativo de TI em SI, etc;d. Indicação de data e hora para o início do teste, e duração. Restrições de horários e datas, devem ser considerados.e. Análise de Risco: Indicação dos riscos, probabilidade e impacto e medidas de mitigação a serem adotadas preventivamente, e plano de contingência;f. Ações de acompanhamento para quando as vulnerabilidades são detectadas.g. Indicação de dados armazenados que podem ser acessados durante o teste.h. Formalização de permissão para realização do teste com as indicações citadas e condicionadas ao código de ética <i>ec-council</i>.i. Em caso de a realização ser efetuado por terceiros, prever também em contrato:<ol style="list-style-type: none">i. As diferentes leis, diretivas ou regulamentos internacionais, nacionais e locais que podem estar envolvidos.ii. Proteção contratual contra responsabilidade.
----	---

#	Diretrizes
	<ul style="list-style-type: none"> iii. Indenização para cobrir resultados de teste incompletos, como vulnerabilidades não encontradas. iv. Garantias através de <i>Non Disclosure Agreement</i> v. Cláusula de eliminação de evidências.
30	<p>Realização do teste de vulnerabilidade:</p> <ul style="list-style-type: none"> a. Iniciar o teste de acordo com o planejado e autorizado, e com as medidas de mitigação de risco executadas; b. Suspender o teste caso algum risco tenha ocorrido e que não tenha medida de mitigação planejada/executada e/ou plano de contingência; c. Colher informações necessárias par realização do teste; d. Investigar o ambiente objeto do teste; e. Explorar as vulnerabilidades possíveis; <p>Identificar as ferramentas utilizadas, dados utilizados, resultados e evidencias da existência/ausência de vulnerabilidade.</p>
31	<p>Finalização e conclusão do teste de vulnerabilidade:</p> <ul style="list-style-type: none"> a. Eliminar qualquer configuração/ajuste que tenha sido realizado na realização do teste (objetiva-se que nada seja deixado em aberto e que possa se tornar em uma vulnerabilidade e ser explorado). b. Elaborar relatório contendo: <ul style="list-style-type: none"> i. O documento do planejamento; ii. O documento de autorização; iii. Descrição do teste identificando ferramentas e dados utilizados; iv. resultados e evidências das vulnerabilidades encontradas ou não; v. Para a vulnerabilidades encontradas, avaliação de risco (probabilidade x impacto); vi. Conclusões; vii. Recomendações para eliminação das vulnerabilidades encontradas e priorização.
32	<p>Eliminação das vulnerabilidades:</p> <ul style="list-style-type: none"> a. Adotar ações para eliminação da vulnerabilidade; b. Evidenciar as ações realizadas; c. Ressaltar as vulnerabilidades para que as ações de eliminação sejam testadas imediatamente após a eliminação ou em um próximo ciclo de testes.
33	<p>Comunicação dos testes de vulnerabilidade:</p> <p>Os relatórios dos testes (tantos os de identificação como os de eliminação) devem ser comunicados à SUPTI, ao Comitê de Segurança da Informação e à DIREXE.</p>
<p>RESTRIÇÕES QUANTO À INSTALAÇÃO DE SOFTWARE</p>	

#	Diretrizes
34	A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) e Manuais, caso aplicável, estabelecendo os critérios para a instalação de <i>software</i> .
AUDITORIA EM SISTEMAS DE INFORMAÇÃO	
35	A SUPTI deve planejar e acordar com a SUPTI as atividades e requisitos de auditoria envolvendo a verificação nos sistemas de forma a minimizar a interrupção nos processos do negócio da Companhia.
36	<p>Para minimizar os impactos das atividades de auditoria em sistemas a SUPTI deve:</p> <ul style="list-style-type: none"> ○ Acordar previamente com a gerência os requisitos de auditoria; ○ Acordar previamente e controlar o escopo dos testes técnicos; ○ Limitar os testes de auditoria para acesso somente de leitura de <i>software</i> e dados; ○ Acessos diferentes de apenas leitura permitidos somente através de cópias isoladas de arquivos de sistemas e dados. Estas cópias devem ser apagadas após a atividade de auditoria, ou dada proteção adequada se existir a obrigação de guarda de tais arquivos para fins de requisitos de documentação de auditoria; ○ Identificar e acordar previamente requisitos de processamento adicional ou especial; ○ Realizar fora do horário comercial testes de auditoria que possam afetar a disponibilidade de sistemas de negócio; ○ Monitorar e registrar todos os acessos de forma a produzir uma trilha de referência.

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	<p>Aplicação das políticas e práticas de Segurança da Informação.</p> <p>Responsável pelos controles tecnológicos que apoiam a proteção da informação de todas as Unidades de Gestão da SPA, nos aspectos de:</p> <ul style="list-style-type: none"> • Identificação; 	N/A

	<ul style="list-style-type: none">• apresentação;• sustentação;• escolha;• implantação; e,• manutenção.	
--	---	--

7.2. Das Unidades Executoras

Área	Atividades	Ferramenta
Gerência de Infraestrutura de Dados (GERID)	Realizar os testes de vulnerabilidade.	várias

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.

Registro de Alterações				
Tópico	Versão	Página	Data	Descrição Sumária