	AUTORIDADE PORTUÁRIA DE SANTOS		
	Instrumento Normativo de Processo		**Código: TIC-020**
	Diretoria Responsável: **Presidência**	Unidade Responsável: **Superintendência de Tecnologia da Informação**	Elaboração: Supervisão de Governança de TI
	Início da vigência: **31/05/2023**	Aprovação: Decisão Direxe **nº 198.2023**	Validação: **Superintendente de Tecnologia da Informação**
PROCESSO: Gestão de Serviços de TIC			Versão: **4.1**

INSTRUMENTO NORMATIVO DE PROCESSO DE GESTÃO DE SERVIÇOS DE TIC

SUMÁRIO

1. OBJETIVO DO PROCESSO

Cobrir as atividades, boas práticas e subprocessos referentes à **Gestão de Serviços de TIC**, passando por todo o ciclo de vida de um Serviço de TIC (definição, implantação, gerenciamento e manutenção), visando a **entrega de valor**, a **segurança e privacidade das informações** e o **atendimento das necessidades de clientes e usuários**.

Os subprocessos de Gestão de Serviços de TIC atualmente mapeados e normatizados na Autoridade Portuária de Santos S.A. ("APS" ou "Companhia") e seus objetivos estão listados a seguir:

I. Suporte (Incidentes e Solicitações de Serviços)

Atendimento satisfatório às demandas dos usuários, mediante o fornecimento de resposta rápida e eficaz às suas solicitações.

II. Incidentes de SI&P

Possibilitar uma resposta rápida e eficaz para o reestabelecimento do ambiente operacional e adoção de outras medidas pertinentes.

III. Níveis de Serviço de TIC

Garantir a padronização dos trabalhos de ciência e concordância dos usuários quanto aos níveis mínimos dos serviços ofertados pela SUPTI.

IV. Gestão de Acessos Lógicos

Garantir que apenas usuários autorizados possuam acesso às informações contidas nos serviços de TIC, de acordo com os requisitos de negócio.

Observação: Conforme o Grau de Maturidade em Gestão de Serviços de TIC evoluir, novos subprocessos podem ser incluídos. Exemplos: Gestão do Portfólio de Serviços de TIC, Gestão de Mudanças, Gestão de Configurações etc.

2. ABRANGÊNCIA

Este normativo se aplica a área de TIC da Companhia e a todos os usuários de recursos e serviços por ela ofertados.

3. FUNDAMENTAÇÃO

Este documento está fundamentado na Política de Gestão de Serviços de TIC da Companhia, na Política de Segurança e Privacidade e no SGPI e nas boas práticas abaixo:

Referência	Descrição
ISO/IEC 27001:2013	*Information technology -- Security techniques -Information security management systems --Requirements*
ISO/IEC 27002:2013	*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-27035:2016	*Information technology — Security techniques — Information security incident management*
ISO/IEC 27701:2019	*Information technology -- Security techniques - Privacy Information Management System (PIMS)* (Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Privacidade da Informação – SGPI)
***Information Technology Infrastructure Library* (ITIL)**	Conjunto de melhores práticas dos processos de gestão de serviços de Tecnologia da Informação (TI) de uma empresa.
SANS	*SysAdmin, Audit, Network and Security*, Instituto especializado em treinamento em segurança da informação, e *cybersecurity*.
NIST	*National Institute of Standards and Technology*, é uma agência governamental não regulatória da administração de tecnologia do Departamento de Comércio dos Estados Unidos

4. DEFINIÇÕES

TERMO	DESCRIÇÃO
Ameaça	Conjunto de fatores externos com o potencial de resultar em dano para um sistema ou organização.
ANO	Acordos de Níveis Operacionais.
ANS - Acordo de Nível de Serviço	É um compromisso firmado entre o Prestador de Serviços de TIC e seus usuários, no sentido de clarificar quais as exigências e condições mínimas ou desejáveis que um determinado serviço precisa atender para ser considerado satisfatório, estabelecendo critérios objetivos para medir a qualidade e o desempenho do Serviço.
Áreas de negócio de TIC	Unidades de gestão subordinadas à Superintendência de TIC que constroem e entregam serviços de TIC. Notadamente as áreas de Infraestrutura e de Desenvolvimento de Software.
Atendimento 1º nível	Atendimento inicial (primeiro contato) aos clientes internos e externos da Companhia para registrar e, se possível, atender remotamente os chamados abertos por meio de procedimentos básicos ou procedimentos registrados na base de conhecimento.
Atendimento 2º nível	Atendimento presencial que visa a execução de procedimentos que necessitam de ação física ou investigação e solução de situações não resolvidas em 1º nível.
Atendimento 3º nível	Atendimento especializado realizado por empregados técnicos do quadro interno ou agentes externos provedores de serviço

	de TI, voltados à solução de incidentes, problemas ou requisições de serviço de alta complexidade ou que exijam alteração nos parâmetros de serviços de TI ainda não registrada na base de conhecimento para solução em 1º ou 2º níveis ou que exijam procedimentos em ferramentas de acesso ao registro. O 3º nível também atua passando instruções ao 1º e 2º nível.
Ativo	Qualquer bem, material ou não, que tenha valor para a Companhia e precisa ser adequadamente protegido.
Base de Conhecimento	Acervo de tutoriais e documentações que serve como base para solução de atendimentos.
Categorização do chamado	Conjunto de categorias, previamente definidas, referente a solicitação do usuário.
Central de Serviços (Service desk)	É a unidade funcional constituída por determinado número de técnicos e recursos, responsáveis por lidar com uma variedade de demandas de serviço de TIC em primeiro e segundo nível, usualmente via chamada telefônica ou interface de web. Esse papel é desempenhado pela Supervisão de Operação e Soluções de TI.
Cliente de Serviços de TI	Cliente é a pessoa responsável por requisitar um Serviço de TIC às Áreas de Negócio de TIC, sendo o definidor de todos os Requisitos de Serviço deste novo ou existente Serviço de TIC. Também é responsável por representar os usuários destes Serviços de TIC junto às Áreas de Negócio de TIC, apresentando comunicações, mantendo diálogo e levando fatos e argumentos quotidianos acerca da rotina de utilização do Serviço de TI pelos Usuários às Áreas de Negócio de TIC.
Conta de Serviço	Contas utilizadas para acessos automáticos à sistemas. Ex: Login para conexão com o Banco de Dados.
Conta Setorial	Contas genéricas que são compartilhadas entre usuários. Ex: presidencia@brssz.com.
CSTIC	Catálogo de Serviços de TIC.
CTIR	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República.
Encarregado pela proteção de Dados Pessoais (ETDP)	Pessoa ou função responsável pela gestão dos dados pessoais tratados pela Companhia, para atuar no canal de comunicação entre o controlador (no caso a APS), o titular dos dados e a ANPD. Esse papel é nomeado via portaria pelo Presidente da Companhia.

Erro conhecido (*Known Error*)	Problema que tem causa raiz documentada e uma solução de contorno identificada.
Escalonamento	Atividade que obtém recursos adicionais quando necessários para alcançar determinado nível de serviço ou expectativa do cliente. O escalonamento pode ser necessário no contexto de qualquer processo de gerenciamento de serviço de TI, porém é mais frequentemente associado com o gerenciamento de incidentes, gerenciamento de problemas ou gerenciamento de requisições de serviços. O escalonamento pode ser dividido em dois tipos: funcional e hierárquico.
Especialistas	Grupo de empregados com conhecimentos específicos, de infraestrutura ou de sistemas, para o atendimento dos chamados encaminhados pelo 1º nível. Geralmente é o grupo composto pelos 2º e 3º níveis.
ETIR	Sigla de Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos. Equivalente aos termos ERI (Equipe de resposta a Incidente), CERT (*Computer Emergency Response Team*) e CSIRT (*Computer Security Incident Response Team*)
Evento	Qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um firewall que faz um bloqueio de uma tentativa de conexão, entre outros.
Evento adverso (ou ofensivo)	Evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de malware que destrói dados, entre outros.
Eventos de segurança da informação	Qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança.
Gerenciamento de problemas	É o processo responsável por gerenciar o ciclo de vida de todos os problemas.
Incidente	Interrupção não planejada de um serviço de TI ou uma redução em sua qualidade, levando-se em consideração o nível de serviços acordado (ANS).
Incidente de Segurança da Informação	Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores. Interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação

	ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
Incidentes de segurança da informação envolvendo dados pessoais	É um incidente de segurança da informação, em que dados pessoais estão dentre os elementos diretamente afetados.
Informação	Conjunto de dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
Item de configuração (IC)	Refere-se a qualquer componente que necessita ser configurado com o objetivo de se entregar um serviço de TI. Os ICs normalmente incluem serviços de TI, hardware, software, pessoas e documentações formais, como documentação de processos e acordos de nível de Serviço.
MFA	A MFA (autenticação multifator) adiciona uma camada de proteção ao processo de entrada. Os usuários fornecem uma verificação de identidade adicional ao acessar contas ou aplicativos, como a leitura de uma impressão digital ou a adição de um código recebido por telefone.
Laudo técnico	Relatório que detalha tecnicamente o atendimento do chamado, com a solução ou justificativa do não atendimento.
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.
Prevenção às violações de dados Pessoais	Ações resultantes de avaliações de impacto dos dados pessoais (Relatório de Impacto à proteção de Dados - RIPD) antes do início de qualquer projeto ou implementação de qualquer tecnologia que processe (tratamento) Dados Pessoais.
Problema	Causa raiz de um ou mais incidentes.
Processo	Conjunto de atividades inter-relacionadas ou interativas que utiliza recursos para transformar insumos (entradas) em produtos (saídas).
Registro de Violação de Dados Pessoais	Coleção de registros de incidentes com violação de dados pessoais que permite identificar tanto os que foram comunicados à ANPD como os que não foram.

Requisição de serviços	É o mecanismo pelo qual o usuário formalmente requisita algo à área técnica provedora de serviços de TI.
Resposta a Incidente	Conjunto de atividades técnicas executadas para analisar, detectar, defender contra um incidente e responder a um incidente. Fonte *https://blog.elearnsecurity.com/security-incidents-incident-handling-vs-incident-response.html*
RIPD	Relatório de Impacto à proteção de Dados
Risco	No sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade.
Senha temporária	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*.
Serviços de TIC	Produto, Serviço ou Item de Serviço de TIC
Segregação de Funções	Consiste na separação de funções, nomeadamente de autorização, aprovação, execução, controle e contabilização das operações.
Sistema de Chamados de TIC	Sistema específico da TIC, de responsabilidade da Central de Serviços, disponibilizado na Intranet da Companhia para a abertura de chamados técnicos relacionados aos ativos de Tecnologia da Informação.
Solução de Contorno (*Workaround*)	Meio temporário de resolver incidentes.
TIC	Sigla de tecnologia da informação e comunicação.
Tratamento de Incidentes	Consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias.

5. ARCABOUÇO LEGAL

Leis, Normativos Externos, Ofícios e Resoluções	Ano	Assunto
Resolução nº 41 CGPAR	2022	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.

NC Nº 05 GSI	2009	Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR.
NC Nº 08 GSI	2010	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais.
NC Nº 21 GSI	2014	Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes.
Decreto Nº 9.637 – PNSI	2018	Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação
Decreto nº 10.748	2021	Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

6. DISPOSIÇÕES NORMATIVAS

6.1. SUBPROCESSO – GESTÃO DE SUPORTE DE TIC

6.1.1. PRINCIPAIS ATIVIDADES– GESTÃO DE SUPORTE DE TIC

ATIVIDADES	REGRAS/DIRETRIZES
ABERTURA DE CHAMADO	1) A **abertura de chamados** deve ser de fácil acesso, tanto pelos usuários internos como externos à Companhia. 2) O primeiro contato sobre incidentes e/ou requisições de serviços sempre deve ser realizado por meio da Central de Serviços (*Service Desk*), tanto para requisitantes internos como externos. 3) Todos os chamados devem ser registrados no Sistema de Gestão de Serviços de TIC, contendo, no mínimo, sua classificação, como requisição ou incidente (inclusive de segurança da informação), categorização e a sua respectiva priorização, tendo como critérios: a) A criticidade de negócios, e; b) Os níveis de serviço acordados.
TRIAGEM DE CHAMADO	4) Os dados do chamado devem ser analisados quanto a qualidade, integridade e suficiência das informações, solicitando-se complemento aos usuários e/ou realizando correções quando necessário. 5) Após análise, o chamado deve ser direcionado ao nível adequado de atendimento. 6) Caso o chamado seja um incidente de natureza grave (de forma a colocar em risco determinado negócio estratégico para a Companhia), os gerentes de TI devem ser tempestivamente comunicados para a adoção de medidas em caráter emergencial. 7) As diretrizes de identificação de eventos e incidentes de SI do subprocesso de Gestão de Incidentes de SI devem ser observadas nessa atividade.
ATENDIMENTO DE CHAMADO	8) O escalonamento do 1º nível para o 2 º nível deve ocorrer quando: a) se atingir tempos-limite para atendimento; b) quando constate não ser possível resolver o chamado em 1º nível. 9) O escalonamento para o 3 º nível deve ocorrer:

	a) em casos de tentativa frustrada de resolução pela Central de Serviços, inexistência de informações na base de conhecimento ou; b) quando a base de conhecimento assim orientar. 10) Independentemente do escalonamento, o *Service Desk* permanecerá responsável pelo acompanhamento do ciclo de vida do chamado, acompanhando o transcorrer dos trabalhos da área técnica, de forma a possibilitar respostas ágeis ao cliente quanto ao status da demanda. 11) Os **chamados** referentes a requisições de serviço que envolvam **perfil de acesso devem ser autorizados pelo cliente do serviço (autorizador)**, conforme procedimentos registrados na base de conhecimento.
CONCLUSÃO DE ATENDIMENTO DE CHAMADO	12) Toda conclusão de atendimento de chamado deve conter diagnósticos da resolução ou laudo técnico. Os diagnósticos deverão levar em consideração: a) Identificação e descrição de sintomas relevantes para estabelecer as causas mais prováveis dos incidentes; b) Referências de fontes de conhecimento disponíveis; c) Se um problema relacionado ou erro conhecido ainda não existir e se o incidente satisfizer critérios de registro de problema previamente acordados, registrar um novo problema; d) Na resolução e recuperação de incidentes, dever-se-á documentar, aplicar e testar as soluções definitivas ou alternativas identificadas e executar ações para restaurar o serviço. 13) Os chamados devem ser fechados somente pelo requisitante, e no prazo máximo de 3 dias da solução do atendimento pela área de TI.
MONITORAMENTO DO PROCESSO	14) O gerenciamento de requisições de serviço e incidentes, bem como o cumprimento do ANS pelo *service desk* devem ser avaliados por meio da medição periódica de indicadores, com foco no aprendizado e melhoria contínua do processo. *15)* O grau de satisfação do cliente interno em relação aos serviços de suporte será acompanhado mediante pesquisa *(feedback*).
GERENCIAMENTO DE PROBLEMAS	16) Todo problema deve ser identificado e aplicada solução de contorno ou, quando possível, correção definitiva.

6.2. SUBPROCESSO – GESTÃO DE INCIDENTES DE SI&P

6.2.1. DIRETRIZES GERAIS – GESTÃO DE INCIDENTES DE SI&P

Os incidentes de segurança da informação devem ter a devida atenção por parte da alta administração da Companhia. Cabe à Autoridade Portuária de Santos garantir que exista estrutura suficiente para prevenir e responder tais incidentes. Por estrutura suficiente entende-se:

I. pessoal, em quantidade e qualificação adequada;
II. recursos de TIC compatíveis com o parque de ativos e grau de segurança esperado;
III. ampla conscientização dos empregados e externos afetados pelos serviços de TIC da Companhia sobre como notificar fragilidades e eventos de SI&P, e;
IV. atuação ativa da alta administração da Companhia no patrocínio e nas tomadas de decisão para viabilização deste subprocesso.

O tratamento de incidentes de segurança da informação é de responsabilidade da ETIR (Equipe de Prevenção Tratamento e Resposta de Incidentes Cibernéticos).

A ETIR tem como missão: a facilitação e a coordenação das atividades de tratamento e resposta a incidentes de SI&P. Incluindo, mas não se limitando à:

I. recuperação de sistemas;
II. análise de ataques e intrusões;
III. cooperação com outras equipes;
IV. participação em fóruns e redes nacionais e internacionais de tratamento e resposta à incidentes de SI&P, como o CTIR.

Os seguintes setores deverão ser representados na ETIR, ao menos com um membro titular e seu suplente:

I. Gestor de Segurança da Informação **(como decisor)**;
II. Segurança cibernética **(como coordenador)**;
III. Segurança da Informação & Privacidade;
IV. Proteção de dados pessoais;
V. Infraestrutura de TI;
VI. Suporte ao usuário (*service desk*);
VII. Desenvolvimento de Sistemas;
VIII. Gestão de riscos e controles internos **(como consultivo)**.

O modelo de implementação seguido para a **ETIR** é o de **uso da própria equipe de TIC**, portanto, **não há dedicação exclusiva as funções** de prevenção, tratamento e resposta à incidentes de SI&P.

Os membros da ETIR deverão ser **formalizados via portaria DIPRE**, sendo sua nomeação de ciência dos participantes e seus gestores, além de previamente aprovada pelo CSI.

A ETIR tem duração permanente cabendo revisão dos membros e escopo de responsabilidades, por parte do CSI, sempre que necessário.

Deve ser mantido pelo setor de Segurança da Informação em conjunto com a GECAR um programa de capacitação em incidentes de segurança da informação para **garantir que a ETIR tenha conhecimento suficiente** para suas funções e que exista conscientização dos funcionários e entes externos que utilizam serviços de TIC da Companhia. Este programa deve fazer parte do Programa Anual de Capacitação do setor de treinamento, sendo de **vital importância que os empregados sejam conscientizados sobre como identificar eventos de SI&P e reportá-los**.

A **ETIR** deve se manter atualizada sobre acontecimentos de segurança cibernética, estabelecendo contato com autoridades, grupos de interesses externos ou fóruns que tratem de questões relativas a incidentes de segurança da informação.

O ponto de contato único estabelecido com a **ETIR** deve ser o e-mail etir@brssz.com. Sendo que, **eventos e incidentes de SI&P devem ser registrados via sistema de chamados de TIC**, conforme subprocesso de Gestão de Suporte.

A **autonomia para tomada de decisão da ETIR** é completa. Ela poderá conduzir o seu público-alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de SI&P. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

A criticidade dos incidentes de segurança da informação deve ser definida de acordo os pilares de SI&P comprometidos:

CENÁRIOS	PILAR DE SI COMPROMETIDO			CRITICIDADE
	C	I	D	
Cenário 1	**SIM**	**SIM**	**SIM**	**ALTA**
Cenário 2	**SIM**	**SIM**	**NÃO**	**ALTA**
Cenário 3	**NÃO**	**SIM**	**SIM**	**ALTA**
Cenário 4	**SIM**	**NÃO**	**SIM**	**ALTA**
Cenário 5	**SIM**	**NÃO**	**NÃO**	**ALTA**
Cenário 6	**NÃO**	**SIM**	**NÃO**	**MÉDIA**
Cenário 7	**NÃO**	**NÃO**	**SIM**	**BAIXA**

Observação: C= Confidencialidade; I = Integridade; D = Disponibilidade.

6.2.2. PRINCIPAIS ATIVIDADES– GESTÃO DE INCIDENTES DE SI&P

ATIVIDADES	REGRAS/DIRETRIZES
PLANEJAMENTO - PREVENÇÃO DE INCIDENTES DE SI&P	**1)** Periodicamente, ao menos **<u>uma vez ao mês, deve ocorrer reunião da ETIR</u>** para tratar da prevenção de incidentes de SI&P. Nesta reunião devem ser pautados assuntos como: a) Discussão e atualização de procedimentos de gestão de incidentes de SI&P (como Plano de Resposta ao Incidente e lista de contatos para comunicação de incidentes de SI&P); b) Apresentação de relatórios de eventos e incidentes de SI&P do último mês; c) Apresentação de problemas e vulnerabilidades encontrados e priorização para atendimento deles; d) Apresentação de indicadores de maturidade e desempenho; e) Definição de ações de melhoria e tratamento para maior prevenção dos incidentes de SI&P; f) Acompanhamento de ações de melhoria e tratamento em andamento; g) Definições ou alterações da ETIR; h) Definições ou alterações da escala de acionamento (*scalation*) no caso de incidente de SI&P; i) Recebimento e análise das atualizações do catálogo dos recursos tecnológicos do parque existente; j) Recebimento e análise das atualizações da priorização de sistemas a ser restaurado em caso de incidente.
MONITORAMENTO E IDENTIFICAÇÃO DE EVENTOS DE SI&P	**MONITORAMENTO** **2)** A ETIR deve monitorar, detectar, analisar e notificar os eventos de segurança da informação a partir de: a) planejamento e análise de ameaças e vulnerabilidades; b) aprimoramento de ferramentas de análise de segurança e listas de verificação; c) melhorias nas regras de monitoramento. **3)** O monitoramento e identificação de eventos de SI&P podem ser realizados: a) de forma proativa pela ETIR, com apoio de ferramentas de segurança (Firewall, Gestão de Eventos, Antivírus etc.), ou;

ATIVIDADES	REGRAS/DIRETRIZES
	b) de forma reativa por qualquer usuário dos serviços de TIC da Companhia ou por fornecedores que acessam informações da Companhia. **IDENTIFICAÇÃO** **4)** As seguintes situações podem caracterizar um evento de SI&P (lista não exaustiva): a) Controles de segurança ineficazes; b) Detecção de qualquer inconsistência com relação à disponibilidade, confidencialidade e integridade (e Privacidade) de qualquer informação da Companhia; c) Alterações sistêmicas sem prévio aviso; d) Hardware ou software com comportamento suspeito; e) Acesso lógico comprometido; f) Violações de segurança física; g) Quaisquer outras ações de inconformidade com as normas de SI&P vigentes. **5)** Identificados os **eventos de SI&P, eles devem ser registrados imediatamente** via sistema de chamados de TIC da Companhia. O registro pode ser realizado por usuário ou fornecedor dos serviços de TIC da Companhia e deve incluir o máximo de informações possíveis para auxiliar o tratamento do evento, incluindo detalhes como: a) qual é a não conformidade ou violação; b) quais são as ocorrências de mau funcionamento; c) evidências como erros, mensagens e recortes de tela. **6)** **Eventos de SI&P podem ser identificados como incidentes de SI&P**. Por conta disso, cada chamado de evento de SI&P deve ser analisado e tratado pela ETIR tomando como base o subprocesso de gestão de Suporte, utilizando-se sempre que possível dos procedimentos vigentes e da base de conhecimento.

ATIVIDADES	REGRAS/DIRETRIZES
	IMPORTANTE!!!: Mesmo que sejam apenas suspeitas, deve-se realizar o registro dos eventos, de modo que a ETIR possa analisá-los e validá-los rapidamente e, uma vez confirmado o incidente de segurança, proceder com uma análise aprofundada. **7)** A criação de uma tabela de respostas rápidas aos incidentes pela ETIR pode auxiliar na identificação e apoio ao primeiro atendimento. **8)** O resultado do tratamento do evento de SI&P deve ser comunicado ao notificante.
IDENTIFICAÇÃO DE INCIDENTES DE SI&P	**9)** Cabe a ETIR avaliar e decidir se um evento de SI&P é caracterizado ou não como incidente de SI&P e se envolve ou não dados pessoais. **Essa avaliação deve ser registrada no sistema de chamados de TIC.** **10)** Havendo uma das seguintes características no evento de SI&P, ele poderá ser classificado como um incidente de SI&P: a) abuso de sítios (desfiguração, injeção de links/código - *spamdexing*, erros de código, cross site scripting, abuso de fórum ou livros de visita etc.); b) inclusão remota de arquivos (*remote file inclusion* - RFI) em servidores web; c) uso abusivo de servidores de e-mail; d) hospedagem ou redirecionamento de artefatos ou código malicioso; e) ataques de negação de serviço; f) uso ou acesso não autorizado a sistemas ou dados; g) varredura de portas; h) comprometimento de computadores ou redes; i) desrespeito à política de segurança ou uso inadequado dos recursos de TIC; j) ataques de engenharia social - *phishing*; k) cópia e distribuição não autorizadas de material protegido por direitos autorais; l) uso abusivo ou indevido de redes sociais para difamação, calúnia, ameaças ou fraudes. **11)** Cabe a ETIR a coleta de evidências forenses e comunicação às autoridades policiais competentes (via DIPRE) nos casos a seguir:

ATIVIDADES	REGRAS/DIRETRIZES
	a) Divulgação não autorizada de dado ou informação sigilosa contida em sistema, arquivo ou base de dados da Companhia, nos termos do art. 153, §1º-A do Código Penal; b) Invasão de dispositivo de TIC, nos termos do art. 154-A do Código Penal; c) Interrupção de serviços de TIC, previsto no §1º do art. 266 do Código Penal; d) Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados da Companhia, nos termos do art. 313- A do Código Penal; e) Modificação ou alteração de software sem autorização por funcionário, nos termos do art. 313-B do Código Penal; f) Distribuição, armazenamento ou conduta vinculada a pornografia infantil, nos termos dos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei nº 8069/90; e g) Interceptação clandestina de comunicações, nos termos do art. 10 da Lei nº 9296/96; **HAVENDO DADOS PESSOAIS** **12)** Em caso de incidente envolvendo dados pessoais, o Service desk deve comunicar ao ETDP, que avaliará um potencial Incidente de Violação de Dados Pessoais. **IMPORTANTE:** Estando os dados pessoais anonimizados, não há violação dos dados pessoais.
TRATAMENTO DE INCIDENTES DE SI&P - PLANEJAMENTO	**13)** Identificado um incidente de SI&P, deve ser realizada **reunião entre a ETIR e quem mais for necessário em Sala de Crise** (*War Room*) para definir as ações cabíveis para o tratamento do incidente. Dependendo do tipo de incidente, não é obrigatória nem necessária a convocação de todos os membros da ETIR. **14)** O coordenador da ETIR deve **centralizar as informações do planejamento de tratamento do incidente** para fornecê-las às partes interessadas como: Gestor de SI&P, Setor de Segurança da Informação, Encarregado de Proteção de Dados, Diretoria e afetados pelo incidente. **15)** Neste momento, o **acesso físico à Gerência de Infraestrutura de Dados deve ser restrito a ETIR, equipe de infraestrutura e envolvidos no incidente autorizados pela ETIR**.

ATIVIDADES	REGRAS/DIRETRIZES
	16) O planejamento das ações para tratamento do incidente de SI&P identificado deve tomar como base: a) os procedimentos definidos para resposta a cada tipo de incidente; b) a criticidade do incidente.; c) os recursos necessários para que a resposta seja efetiva, mesmo que provisória.
TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VALIDAÇÃO	**17)** O tratamento de incidentes de SI&P deve visar: a) Sua contenção, isolando ativos afetados para prevenir danos maiores; b) Sua erradicação, eliminando a causa raiz; c) A recuperação, colocando ativos afetados em condições normais de funcionamento. **IMPORTANTE:** Deve ser priorizado o reestabelecimento da segurança antes de efetuar a recuperação. **18)** Durante o incidente (**RESPOSTA**) a. Coletar **evidências, o mais rápido possível** após o evento; b. Conduzir **análise forense** de segurança da informação **(quando aplicável)**; c. Disponibilizar as ferramentas e recursos para as atividades de recuperação (*backups* para *restore*, atualizações de antivírus, *patches* de correções etc.). d. Escalar, se requerido; e. **Registrar as atividades** de respostas para análise futura; f. **Notificar o CTIR**; g. **Comunicar** a existência do incidente de segurança da informação ou violação de **dados pessoais** para pessoal interno ou externo, ou organizações que precisam tomar conhecimento do fato; h. Avaliar riscos de violação de **dados pessoais**, quando aplicável; i. **Instruir afetados** sobre medidas corretivas a serem tomadas; j. **Tratar das fragilidades** de segurança da informação encontradas que causaram ou contribuíram para o incidente.

ATIVIDADES	REGRAS/DIRETRIZES
	IMPORTANTE: De modo a facilitar a tomada de decisão, uma relação de quais partes interessadas devem ser contatadas para cada tipo de incidente ou serviço de TIC afetado deve ser mantida. A lista pode conter: empregados da Companhia, funcionários terceirizados, seguradoras, agentes da lei, agências/órgãos governamentais, CTIR Gov, CERT.br etc. **19)** Após o incidente a ETIR deve: (**VALIDAÇÃO**) a. **Realizar validações** (pente fino) em toda a estrutura afetada ou não, para garantir que o ambiente está seguro para utilização. b. Buscar **identificar sua origem**; c. Sugerir a criação de um **processo disciplinar** formal conforme procedimentos correcionais em vigor, direcionado a quem violou as normas de SI&P; d. Registrar lições aprendidas; e. Encerrar, analisar e registrar o incidente uma vez que ele foi tratado de forma bem-sucedida.
AVALIAR VIOLAÇÃO DE DADOS PESSOAIS	**20)** A avaliação deve ser conduzida com participação dos responsáveis pela gestão dos dados violados com apoio do ETPD. **21)** Deve-se determinar se existe um risco para os direitos e liberdades dos titulares dos dados. Os riscos contra os direitos e liberdades incluem, entre outros: a. perda de controle ou confidencialidade dos Dados Pessoais; b. reversão não autorizada de pseudonimização; c. danos à reputação, discriminação, roubo ou fraude de identidade; d. perda financeira e outras desvantagens econômicas ou sociais. **22)** O ETPD deve avaliar se a probabilidade e o impacto dos riscos potenciais os configuram como altos. Esta avaliação deve considerar: a. Os dados pessoais envolvidos e seus tipos(sensibilidade); b. O tipo de violação; c. A natureza dos dados pessoais violados; d. Volume de dados pessoais afetados; e. Os danos a direitos do titular de dados pessoais;

ATIVIDADES	REGRAS/DIRETRIZES
	f. O número e as características dos titulares de dados afetados; g. Em caso de vazamento: Informações que um terceiro pode extrair a partir do que foi vazado; h. Se é possível identificar todos os envolvidos na violação de dados ocorrida. i. Se há informações de cadastro/contato de todos os envolvidos na violação de dados ocorrida. **23)** Além do resultado da avaliação, também são riscos elevados os decorrentes de processamento que utiliza novas tecnologias ou métodos de processamento onde nenhuma avaliação de impacto na proteção de dados (RIPD) foi realizada pelo controlador antes da violação, ou quando uma avaliação de impacto nos dados (RIPD) se tornou necessária à luz do tempo decorrido desde o processamento inicial. **24)** Identificados riscos de ordem relevante, o ETPD deve realizar comunicação à ANPD e aos titulares dos dados pessoais.
REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P	**25)** As atividades de gerenciamento de incidentes de SI&P devem ser documentadas observando-se as seguintes informações, quando couber: **INFORMAÇÕES DE CONTROLE E CONTATO** a) Número de controle da ocorrência; b) Nome do coordenador da ETIR, e informações de contato; c) Identificação da APS com sua localização e informações de contato; d) O nome do responsável pela preservação dos dados do incidente, com informações de contato. **INFORMAÇÕES SOBRE O INCIDENTE** e) Descrição do incidente; f) Setor onde ocorreu o incidente; g) Como foi detectado; h) Quem reportou; i) Equipe de resposta; j) Data do evento / Data de identificação; k) Data/hora prevista da solução;

ATIVIDADES	REGRAS/DIRETRIZES
	l) Data/hora da solução; m) Lista de comunicação (pessoas etc.). **DIAGNÓSTICO E TRATAMENTO** n) Natureza do incidente (perda de serviços ou ativos (indisponibilidade), uso indevido de credenciais, violação ou tentativa de burla dos sistemas e controles, observação ou suspeita de fragilidade, acesso indevido, outros); o) Causa raiz identificada; p) Ativos afetados; q) Impacto; r) Providências tomadas para investigação e setores envolvidos; s) Causa raiz resolvida. **EVIDÊNCIAS** t) Dados coletados e preservados e outros dados relevantes; u) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança; v) Número de lacre de material físico preservado, se houver; e w) Justificativa sobre a inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados. **VIOLAÇÃO DE DADOS PESSOAIS** x) A descrição da natureza dos dados pessoais violados; y) As informações sobre os titulares envolvidos; z) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; aa) Os riscos relacionados ao incidente (conforme atividade “Avaliar Violação de Dados Pessoais”); bb) Justificativa de registro e comunicação tardia;

ATIVIDADES	REGRAS/DIRETRIZES
	cc) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo; dd) Identificação de pontos de contato para maiores detalhes; ee) Descrição de possíveis consequências do incidente de violação de dados. ff) Anotação da data da comunicação do incidente à ANPD se houver necessidade de comunicação. Obs.: Os incidentes desta seção, constituem o "Registro de Violação de Dados Pessoais"
COLETA E MANUSEIO DE EVIDÊNCIAS FORENSES	**26)** Com o propósito de investigar os incidentes de SI&P e **responsabilizar condutas ilícitas** que danifiquem ou exponham a segurança e privacidade das informações, devem ser coletadas e manuseadas evidências forenses. **27)** Durante o processo de tratamento do incidente de SI&P, deve-se, sem prejuízo de outras ações, coletar e preservar: a) As mídias de armazenamento dos dispositivos afetados; e b) Todos os registros de eventos (logs) dos serviços de TIC afetados, conforme regramentos vigentes de gestão de operações. **28)** Nos casos em que seja inviável preservar as mídias de armazenamento, em razão da necessidade de pronto restabelecimento do serviço afetado, deve-se coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: Logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os "metadados" desses arquivos, como data, hora de criação e permissões. **29)** Constar em relatório a impossibilidade de preservar as mídias afetadas e listar todos os procedimentos adotados. **30)** **As ações de restabelecimento do serviço não devem comprometer a coleta, e preservação da integridade das evidências**. **31)** Para a preservação dos arquivos coletados, deve-se: a) Gerar um arquivo contendo a lista dos resumos criptográficos de todos os arquivos coletados; b) Gravar os arquivos coletados, acompanhado do arquivo com a lista dos resumos criptográficos descrito na alínea anterior; e c) Gerar o resumo criptográfico do arquivo citado na alínea "a" deste item. **32)** O material coletado deve contar com **avaliação do corpo jurídico da Companhia para identificar as consequências legais do ocorrido e quais autoridades devem ser comunicadas**;

ATIVIDADES	REGRAS/DIRETRIZES
	33) Todo material coletado deverá ser lacrado e custodiado pelo coordenador da ETIR, o qual deve **preencher Termo de Custódia dos Ativos de Informação relacionados ao Incidente de SI&P**. O material coletado ficará à disposição da autoridade comunicada, a qual orientará quanto à sua destinação (ver atividade "**COMUNICAR AUTORIDADES POLÍCIAIS COMPETENTES**").
NOTIFICAÇÃO AO CTIR	**34)** A ETIR deve comunicar o CTIR, a partir de seu e-mail centralizador (etir@brssz.com), seguindo os padrões para notificação de incidentes de segurança ao CTIR, conforme publicado em site próprio do governo. **35)** As notificações ao CTIR via e-mail devem conter: a) **Assunto:** fazer constar o "nome do órgão" e o "tipo do incidente"; b) **Destinatário:** ctir@ctir.gov.br; c) **CC:** eventualmente, podem ser copiados outros envolvidos no incidente; d) **Corpo da Notificação e anexos:** Detalhar o incidente conforme atividade: **REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P**; e) **Observação:** No caso de *phishing* recebido por e-mail, solicita-se que, além do texto da mensagem, sejam enviados os cabeçalhos completos para que se proceda, dentre outras coisas, à notificação do servidor de e-mail comprometido. **36)** A notificação ao CTIR tem o propósito de permitir que o centro preste seus serviços relacionados ao tratamento de incidentes, como: a) tratamento de incidentes; b) análise de artefatos maliciosos; c) coordenação nas respostas a incidentes; d) distribuição de alertas e recomendações; e) estatísticas relativas a incidentes.
COMUNICAÇÃO ÀS AUTORIDADES POLÍCIAIS COMPETENTES	**37)** Após a conclusão do processo de coleta e preservação das evidências do incidente, o coordenador da ETIR deverá enviar relatório com o **REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P** para comunicação às autoridades policiais competentes.

ATIVIDADES	REGRAS/DIRETRIZES
	38) O relatório deverá ser acondicionado em **envelope lacrado e rubricado pelo coordenador da ETIR**, protocolado e encaminhado formalmente ao Presidente da Companhia. **39)** Após receber a comunicação, **o Presidente deve, de imediato, encaminhá-la formalmente à autoridade** com atribuição para apurar os fatos. A comunicação deverá ser acompanhada de envelope lacrado contendo o relatório **40)** **A comunicação** desse relatório, tanto para o Presidente, como para a autoridade responsável, **deve apenas fazer menção de que se trata de comunicação de evento relacionado à segurança da informação**, sem a descrição dos fatos. **41)** A preservação da privacidade e sigilo dos dados custodiados deverá ser observada durante todo o processo de coleta das evidências do incidente de segurança em redes computacionais, na elaboração do relatório, bem como quando do seu envio às autoridades competentes, conforme legislação vigente.
COMUNICAÇÃO DA VIOLAÇÃO DE DADOS PESSOAIS	**COMUNICAÇÃO À ANPD** **42)** Uma violação dos dados que represente risco relevante aos direitos e liberdades das pessoas físicas deve ser relatada à ANPD sem demora injustificada, dentro de **até 48 horas depois** que a Autoridade Portuária de Santos tomar conhecimento da violação, ou em outro prazo definido pela ANPD, se menor. Quaisquer possíveis **motivos para demora na comunicação devem ser informados à ANPD**. A comunicação deve ser realizada obedecendo-se os meios e ferramentas disponibilizadas pela ANPD. **43)** A Companhia é considerada ciente de uma violação de dados pessoais quando existe um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento dos dados pessoais. A Companhia também é considerada ciente quando um operador é informado. **44)** **Um aviso parcial e incompleto deverá ser enviado para a ANPD**, dentro do prazo previsto, **em casos de ocorrência de violações complexas que requeiram investigações detalhadas**, ou quando ocorrerem várias violações semelhantes em um curto período. **45)** As informações mínimas que devem ser enviadas à ANPD constam na seção de "**VIOLAÇÃO DE DADOS PESSOAIS**" da atividade de "**REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P**". **COMUNICAÇÃO AOS TITULARES DOS DADOS PESSOAIS**

ATIVIDADES	REGRAS/DIRETRIZES
	46) Quando a violação oferecer um risco classificado como alto para os titulares de dados e pessoas afetadas, deve-se **elaborar plano de comunicação aos titulares de dados e pessoas** envolvidas no incidente. a) O plano deve ser elaborado com participação do ETPD, Superintendência Jurídica (SUJUD) e Superintendência de Comunicação Corporativa (SUCOC) e aprovado extraordinariamente pelo CSI. b) Esse processo deve ser executado sem demora injustificada. **47)** A comunicação para o(s) Titular(es) dos dados pessoais deve ser produzida em linguagem clara e simplificada e conter, no mínimo, as informações contidas na seção de "**VIOLAÇÃO DE DADOS PESSOAIS**" da atividade "**REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P**". **48)** A comunicação com os titulares dos dados deve ser entregue em mensagens personalizadas individuais, por meios que maximizem as chances de comunicação das informações a todos os titulares dos dados afetados, isso pode exigir a utilização de vários métodos de comunicação e o fornecimento de informações em formatos e idiomas alternativos, se necessário. **49)** Se a violação afetar um grande volume de registros de titulares de dados e dados pessoais, o ETPD decidirá se uma notificação pública em massa é apropriada em vez de uma notificação personalizada individual com base em uma avaliação da quantidade de recursos necessários para notificar cada titular de dados individualmente e sobre a capacidade da APS de fornecer adequadamente aos titulares dos dados a notificação dentro do prazo especificado. **COMUNICAÇÃO AO CONTROLADOR – APS NA CONDIÇÃO DE OPERADOR** **50)** Se os dados pessoais envolvidos no incidente estiverem sendo tratados pela APS, na qualidade de operador, o controlador dos dados deverá ser comunicado sem demora injustificada, devendo a Companhia cooperar com as informações necessárias, bem como com as autoridades fiscalizadoras, para a mais breve apuração, esclarecimento e solução do caso com total transparência.

6.3. SUBPROCESSO – GESTÃO DE NÍVEIS DE SERVIÇOS DE TIC

6.3.1. DIRETRIZES GERAIS – GESTÃO DE NÍVEIS DE SERVIÇOS DE TIC

I. Todo o serviço de TIC deve ter seus níveis mínimos de atendimento acordados por meio de um ANS;

II. Os índices de ANS, suas versões preliminares ou alterações devem ser formalizados entre o Cliente e a Área de TIC responsável pela prestação do serviço;

III. Durante a concepção, planificação e desenho inicial de cada novo Serviço de TIC, deve-se apresentar uma prévia dos níveis mínimos de atendimento;

IV. Durante a implantação efetiva do novo serviço de TI, os índices previamente definidos durante a fase de concepção do novo serviço de TI devem ser revisados e formalizados junto ao cliente em um ANS;

V. **A formalização dos índices de ANS é condição obrigatória para inclusão do serviço no CSTIC durante a transição para a fase de operação e sustentação;**

VI. Os índices de ANS devem ser atualizados junto aos Clientes de TIC de forma anual.

6.3.2. PRINCIPAIS ATIVIDADES– GESTÃO DE NÍVEIS DE SERVIÇOS DE TIC

ATIVIDADES	REGRAS/DIRETRIZES
DETERMINAÇÃO DAS INFORMAÇÕES DO ANS	**1) Descrição do Serviço de TIC:** Incluir quais as funções de negócio que ele abarca, quais os entregáveis deste novo ou existente Serviço de TIC, e a descrição deste Serviço em relação à sua quantidade estimada de usuários, e à escala, impacto, criticidade e prioridade para o negócio. **2) Definição das responsabilidades entre as partes interessadas:** Quais papéis e tarefas esperadas de cada parte, e a identificação dos papéis-chave, tais como o Provedor do Serviço de TIC, o Cliente do Serviço de TIC, e os usuários envolvidos. **3) Definição do Escopo do ANS:** O que está contemplado e o que está excluído do ANS deste Serviço de TIC, incluindo quais as funcionalidades que serão cobertas dentro dos índices acordados de ANS. **4) Definição de horário de funcionamento exigido do Serviço de TIC:** Incluindo (ou excluindo) sábados, domingos e feriados, horário diurno ou noturno, e requisições de extensões especiais de serviço para datas/horas especiais (caso sejam necessárias). **5) Definição de horário de funcionamento do atendimento de suporte aos usuários do Serviço de TIC:** incluindo (ou excluindo) sábados, domingos e feriados, horário diurno ou noturno, e requisições de extensões especiais do auxílio aos usuários para datas/horas especiais (caso sejam necessárias). **6) Disponibilidade mínima exigida:** Disponibilidade mínima exigida (ou indisponibilidade máxima admitida) do Serviço de TIC dentro do horário de funcionamento exigido do Serviço de TIC. **7) Critérios de Segurança:** Incluindo, normas de SI&P que serão contempladas no serviço, regramento para registros de auditoria (logs) e perfis de acesso.

FORMALIZAÇÃO DO ANS	**8)** As Áreas de Negócio de TIC devem apresentar ao Cliente de um novo Serviço de TI as seguintes opções padrão de ANS: a) **Confiabilidade exigida do Serviço de TIC** que, caso seja diferente da Confiabilidade padrão da infraestrutura planejada para o Serviço de TIC, pode ser expressa em número máximo de quebras de serviço aceitas dentro de um determinado período (por exemplo, quebras máximas de serviço dentro de um mês) ou em tempo médio entre falhas/incidentes de serviço; b) **Performance exigida do Serviço de TIC**, tal como velocidade de tarefas específicas, tempos de resposta médio de cada posto de trabalho, ou tempo de execução de tarefas de lote, se houverem ou se exigido pelo Cliente; c) **Especificar se o Cliente do Serviço de TIC em questão aceita a condição atual** dos Planos de Continuidade de TIC, ou se requer um Plano de Continuidade específico para o novo Serviço de TIC, com a previsão de tratamento dos índices de ANS dentro deste Plano para as situações operacionais excepcionais (isto é, desastre, greve, situações de força maior ou de ataque informático) que sejam desejadas pelo Cliente. i) Este Plano de Continuidade deverá ter aderência aos Planos de Continuidade de Negócios da Companhia; ii) Deve incluir os arranjos operacionais que os usuários fariam caso a situação operacional se desenvolva, a definição de quem acionaria o Plano de Emergência, e; iii) Deve nomear os atores responsáveis pela restauração de cópias de segurança do servidor e das estações de trabalho (se aplicável), guarda de dados fora do site, e da realização e suporte operacional à operação de recuperação do desastre (criação de usuários de emergência, mudanças de senhas, ligação de máquinas em site alternativo etc.), quando da ocorrência da situação excepcional. **9)** Os Serviços de TIC existentes no CSTIC devem ser avaliados para que sejam adaptados a passar pelo mesmo processo de formalização descrito pelas diretrizes de 1 a 7, sendo que, a depender desta avaliação, podem ser dispensados deste processo. Esta avaliação deverá ser formalizada junto ao Cliente do Serviço de TIC. **10)** Caso não haja aceitação do Cliente para os padrões de ANS sugeridos, a recusa deve ser formalizada.

MONITORAMENTO E REVISÃO DOS ANS	**11) Manter registro de avaliação de clientes e usuários para melhoria dos processos:** Um registro das reclamações e elogios dos clientes e usuários deve ser mantido a fim de apoiar a melhoria dos serviços e o processo de revisão e formalização dos índices de ANS. **12) Fatores que devem ser observados durante o processo de revisão de índices de ANS:** a. A disponibilidade geral do Serviço de TI; b. A satisfação de seus clientes e usuários; c. A atual capacidade e desempenho da área de TIC em prestá-lo; d. A medição histórica dos níveis de atendimento; e. O histórico de reclamações e elogios, e; f. As expectativas de negócio vigentes e futuras. **13) Medir performance dos serviços mensalmente com relação:** a. Ao atingimento do ANS de cada serviço; b. Ao diagnóstico de principais causas de não atingimento das metas de ANS, e; c. À análise de tendências no desempenho de nível de serviço, para a tomada de ações preventivas. **14) Formatar e divulgar relatório:** a. A performance citada na diretiva anterior deve ser formatada em relatório que deve ser amplamente divulgado e, no mínimo, contemplar visões para o Comitê de TI, os Clientes e Usuários de cada Serviço de TIC.
DEFINIÇÃO DO ANO	**15) Firmar índices de ANO com parceiros internos e prestadores de serviços:** Índices de ANO devem ser firmados com parceiros internos ou prestadores de serviço que fornecem suporte/sustentação aos Serviços de TIC prestados aos Clientes, caso sejam convenientes para uma melhor performance do Serviço de TIC. Esses índices de ANO devem ser atrelados às metas de desempenho do(s) serviço(s) a ser(em) sustentado(s). **16) Tratar os índices de ANO no mesmo formato dos índices de ANS:** Os índices de ANO que sejam formalizados com prestadores de Serviços de TIC devem ser tratados como se fossem ANS do contrato firmado com o Contratado.

	17) **Planejar inclusão dos índices de ANO como parte do ANS:** Um planejamento deve ser efetuado para que os índices de ANO possam ser incluídos como parte do ANS do contrato com o prestador de serviço.

6.4. SUBPROCESSO – GESTÃO DE ACESSO LÓGICO

6.4.1. DIRETRIZES GERAIS – GESTÃO DE ACESSO LÓGICO

Os acessos aos serviços de TIC devem ser gerenciados de forma centralizada pela Central de Serviços.

Conforme características do negócio, algumas atividades do processo podem contar com participação de outras unidades de gestão da Companhia ou empresas contratadas. As atividades podem ser a definição de perfis, a análise da requisição de acesso e a liberação de acesso. Ex.: R.H gerenciando os acessos da ferramenta de treinamentos.

A Gestão de Acesso Lógico deve buscar:

QUALIDADE NO ATENDIMENTO

I. Responder de forma eficiente e apropriada às requisições de liberação, mudança ou revogação de acesso aos serviços de TIC.

ALINHAR-SE AO NEGÓCIO

I. Revisar regularmente as contas;
II. Manter os direitos de acesso alinhados aos requisitos de negócio;
III. Alinhar o gerenciamento de perfis e direitos de acesso aos papéis e responsabilidades exercidos;
IV. Participação ativa dos clientes.

SEGURANÇA DAS INFORMAÇÕES

I. Conceder o mínimo de acesso possível. Restringir antes de liberar: Apenas o necessário e justificável/aprovado será liberado;
II. Identificar de forma única todas as funções de processamento de informações;
III. Considerar a classificação das informações, inclusive pessoais, dando seu devido tratamento e proteção;
IV. Providenciar ajustes e correções que se fizerem necessários nos acessos de modo que a confidencialidade das informações contidas nos serviços de TIC sejam protegidas;

RASTREABILIDADE E PREVENÇÃO DE AÇÕES INDEVIDAS

I. Segregar acessos privilegiados (ex: administrador) de acessos comuns;
II. Observar se os acessos aos serviços estão sendo utilizados de maneira apropriada;
III. Monitorar e gerenciar mudanças de acesso (criação, modificações e remoções);
IV. Manter trilhas de registros de auditoria de acesso, principalmente para informações sensíveis, buscando rastreio de uso abusivo de direitos de acesso;
V. Reduzir erros consequentes de acesso indevido no uso dos serviços de TIC (e.g deleção não intencional de dados por usuário inexperiente), e;
VI. Garantir que todos os usuários de serviços de TIC e suas ações sejam identificados de forma única.

6.4.2. CREDENCIAIS DE ACESSO

Todos os serviços de TIC, dentro do possível e conforme necessidade de proteção das informações, devem ter seu acesso restrito. A restrição deve se dar por meio de credenciais de acesso e pode utilizar métodos de autenticação, como login/senha, biometria, tokens, 2FA/MFA, captcha etc.

As credenciais de acesso são pessoais e intransferíveis, permitindo de maneira clara e inequívoca o reconhecimento do usuário.

SERVIÇOS DE TIC DEVEM

I. encerrar sessões após tempo determinado, principalmente em locais de alto risco (públicos, externos ou móveis), e;
II. ter tempos de conexão restrito, caso seja um serviço de alto risco.

SERVIÇOS DE TIC NÃO DEVEM

I. emitir mensagens que podem auxiliar acesso não autorizado, como informar qual parte está errada na tentativa de login;
II. Mostrar senhas digitadas, a não ser que explicitamente solicitado pelo usuário, e;
III. transmitir senhas em texto claro pela rede.

6.4.2.1. SENHAS

Boas práticas na definição de senhas:

I. não utilizar números sequenciais ou palavras completas;
II. não ser genérica;
III. alterar a senha a cada 180 (cento e oitenta) dias;
IV. não conter informações fáceis de se obter por meio de engenharia social, como datas de aniversário, nome de parentes etc., e;
V. utilizar MFA, quando possível, para:
   A. Acesso remoto/externo à rede ou serviços de TIC da APS, e;
   B. Contas de administração.

Senhas não devem, DE MANEIRA ALGUMA, ser:

VI. utilizadas por qualquer outro usuário, sob qualquer pretexto;
VII. compartilhadas ou cedidas a empresas coligadas, parceiros, superiores, subordinados pessoalmente ou por qualquer outro meio, e;
VIII. divulgadas ou disponibilizadas por qualquer meio de comunicação (excetuando-se senhas temporárias de uso único).

6.4.2.2. CONTAS ESPECIAIS

Contas especiais são aquelas que possuem características específicas que as diferenciam de contas utilizadas pelos usuários comuns dos serviços de TIC.

As diretrizes gerais de Gestão de Acesso Lógico e de Credenciais de Acesso se aplicam às contas especiais.

CONTAS DE ADMINISTRAÇÃO

Contas de administração devem ser utilizadas estritamente **para funções de administração**. Rotinas como acesso à e-mails, navegação na internet, utilização dos serviços de TI em si, devem se restringir às contas comuns. Nesse caso, um empregado que exerça papeis de administração e uso do mesmo sistema terá duas contas.

Deve-se evitar que apenas um usuário possua privilégios de administrador, porém, também é recomendável que não sejam concedidos acesso de administração à um grande grupo de usuários. **Um limite de 5 administradores por serviço de TIC é recomendável.**

Para instalação de serviços de TIC (como aplicações, S.Os e servidores), a fim de evitar acessos indevidos, **são obrigatórias**:

I. a desativação dos usuários nativos, e;
II. a criação de novos usuários administradores.

Na impossibilidade de desativação dos usuários nativos, **a senhas devem ser alteradas no momento da instalação**.

CONTAS DE SERVIÇO

Contas de serviços devem ser utilizadas exclusivamente para automatização de processos.

O uso das contas de serviço deve se restringir às áreas de negócio de TIC.

CONTAS SETORIAIS

Deve haver identificação de quais pessoas acessam e gerenciam contas setoriais, bem como seu responsável.

A gestão de perfis, grupos ou páginas autogeridas em ambientes internos como os disponibilizados em ferramentas de escritório (exemplo: teams, sharepoint, rainbow, etc) **não fazem parte do escopo de gestão da Central de Serviços**, a não ser que sua criação e uso implique no consumo de recursos como licenças de software.

Apesar disso, as práticas deste processo podem ser seguidas por quem os gerir. Ademais, o uso destas contas está sujeito as obrigações determinadas no normativo de "Uso aceitável de Ativos de TIC" da Companhia.

CONTAS DE ACESSO TEMPORÁRIO

É possível conceder acessos temporários para execução de **trabalhos com tempo determinado** nos serviços de TIC **ou em situações de transição**, como transferências ou desligamentos de empregados. O acesso pode ser feito por: empregados da APS, terceirizados, auditores, autoridades ou outros.

Acessos temporários **devem ter data de expiração** e **suas prorrogações justificadas**, formalizadas e aprovadas pelo Cliente contida no serviço de TIC.

Deve ser dada **atenção** para acessos temporários em situações de transição de modo que se **evite o conflito de interesses**.

6.4.3. PRINCIPAIS ATIVIDADES– GESTÃO DE ACESSOS LÓGICOS

ATIVIDADES	REGRAS/DIRETRIZES
INVENTARIAR CONTAS	**1)** Um **inventário de todas as contas** dos serviços de TIC deve ser mantido pela Central de Serviços; **2)** A elaboração do inventário deve cobrir, ao menos: a) **Todos os tipos de usuários,** com identificação única (ex: usuários comuns, administradores e contas de serviços, sejam eles internos, externos ou temporários); b) **Todos os serviços de TIC e sistemas de autenticação**, como aplicações de negócios, aplicações de infraestrutura, sistemas operacionais, aplicações de desenvolvimento e manutenção de sistemas, fechaduras, integrações, APIs etc.; c) Identificação de todos os usuários com pelo menos: i) Nome; ii) Login; iii) Início do período de acesso; iv) Fim do período de acesso; v) Última utilização do serviço; vi) Situação da Conta (ativa, inativa, suspensa etc.); vii) Unidade de gestão, e; viii) Perfis atribuídos. d) Identificação de todas as contas de serviço por: i) Departamento que utiliza; ii) Data de revisão do acesso, e;

ATIVIDADES	REGRAS/DIRETRIZES
	iii) Propósito de uso. **3)** O inventário deve ser revisado conforme estipulado em **"Revisar contas e Perfis"**.
DEFINIR PERFIS	**4)** Perfis de acesso dos usuários, devem ser **definidos e aprovados em conjunto com o Cliente**, com base nos requisitos de negócio. **5)** Deve-se dar preferência à criação de perfis genéricos e identificar exceções/personalizações conforme necessidades, que devem ser justificadas e aprovadas pelo Cliente. **É recomendado buscar um limite de 5 perfis por serviço de TIC.** **6)** Os serviços de TIC devem possuir, ao menos, um perfil de acesso básico e outro de administração. **7)** Serviços onde não é possível criar contas/perfis de acesso, devem ser disponibilizados apenas para quem pode acessar todo seu conteúdo. **8)** Deve-se definir permissões do tipo "ler, escrever, excluir, alterar e executar" para funções/módulos dos serviços de TIC para cada usuário. **9)** **As regras para atribuição de perfis** e condições pré-determinadas de liberação de acesso para cada serviço de TIC **devem ser documentadas,** em conjunto com os ANSs, conforme subprocesso **"Gestão de Níveis de Serviços de TIC",** e **utilizadas para agilizar as requisições de liberação de acesso**. **10)** **É crucial prevenir o conflito de interesses** com separação de funções. Atribuir papéis como de requisição, autorização e administração para pessoas distintas. Exemplos de funções conflitantes: a) Papel 1: Requer acesso à uma informação. Papel 2: Concede acesso à informação; b) Papel 1: Reporta informações de horas extras trabalhadas. Papel 2: Aprova o pagamento de horas extras. **11)** Os perfis devem ser revisados conforme estipulado em **"Revisar contas e Perfis".**
REQUISITAR ACESSO OU ATUALIZAÇÃO DE ACESSO	**12)** Preferencialmente, os serviços de TIC devem conter autosserviço para a requisição ou atualização de acessos.

ATIVIDADES	REGRAS/DIRETRIZES
	13) Alternativamente, uma requisição de acesso pode ser feita por qualquer pessoa, sendo registrada como chamado, seguindo os regramentos de **"Gestão de Suporte de TIC"**. A requisição de acesso pode englobar: a) A criação de uma nova conta; b) A criação/reativação de uma conta temporária; c) A reativação de uma conta; d) A alteração de uma senha; e) A desativação de uma conta (remoção de acesso), ou; f) A transferência da gestão de uma conta de serviço. **14)** Os usuários devem ser instruídos sobre o regramento de requisições de acesso e devem fornecer sua justificativa de necessidade de acesso no chamado registrado. **15)** Registrada a requisição, deve-se prosseguir para sua análise. **ATENÇÃO:** É recomendado automatizar a liberação e revogação de acessos com base no processo de admissão, transferência de setor/função ou desligamento.
ANALISAR REQUISIÇÃO DE ACESSO	**16)** Com as informações da requisição de acesso ou da sua atualização registradas, a Central de Serviços deve buscar pela confirmação de duas condições por parte do requisitante: a) se ele é quem diz ser (pessoa e função), verificando credenciais como: i) Login/senha; ii) Documentação pessoal; iii) Procuração; iv) Certificado;

ATIVIDADES	REGRAS/DIRETRIZES
	v) etc. b) se ele tem legítimo direito de solicitar liberação, atualização ou remoção de acesso ao serviço requisitado, a partir de evidências como: i) Confirmação de contratação pela GEASO em caso de novo empregado; ii) Confirmação de promoção ou transferência pela GEASO; iii) Relação direta e clara da função do requisitante com um dos perfis de acesso pré-determinados ou com a motivação do pedido; iv) Política, norma, lei ou similar que justifique claramente a necessidade de acesso, ou; v) Aprovação do Gestor Imediato do Requisitante e do Cliente, caso nenhuma das condições anteriores estejam presentes. **17) O acesso só deve ser liberado ou removido quando as duas condições acima forem atingidas.**
LIBERAR ACESSO	**18)** A liberação consiste das atividades necessárias para disponibilização do acesso ao requisitante, podendo englobar: a) Configuração/instalação da aplicação; b) Criação efetiva da conta; c) Atribuição de licenças; d) Atribuição/personalização de perfis; e) Geração de senhas; f) Ativação da conta, e; g) Entrega das credenciais. **19)** Quando possível, **toda liberação de acesso**, independentemente do tipo de requisição (nova conta, reativação, transferência etc.), **deve contar com a geração automatizada de uma senha temporária e aleatória**. Essa senha deve ser enviada/comunicada de forma segura e, **após o primeiro acesso, deve ser substituída pelo usuário**.

ATIVIDADES	REGRAS/DIRETRIZES
REMOVER ACESSO	**20)** A remoção de acesso ocorre quando: a) Um empregado é desligado ou deixa de exercer uma função; b) Um acesso temporário expira; c) O usuário estará temporariamente ausente; d) Há um processo de investigação; e) Um processo disciplinar é aplicado; f) Ocorrem 3 falhas seguidas de tentativa de acesso; g) Uma solicitação de remoção é aprovada pelo Gestor do Usuário e o Cliente, ou; h) A conta não é acessada por 45 dias ou mais. **21) A remoção de acesso não significa deleção da conta.** As contas **devem ser mantidas inativas** de modo que possam ser mantidos registros históricos ou para que possa ser reativada no futuro, caso necessário. **Não é permitido o reaproveitamento de credenciais por outras pessoas que sejam a própria dona.**
MONITORAR ATIVIDADES DAS CONTAS	**22) Registros sobre as atividades de usuários**, bem como do gerenciamento e administração de contas em si, **devem ser mantidos**, com identificação mínima do usuário, IP, data e hora do acesso ou ação. **23)** Esses registros devem ser mantidos **por pelo menos 6 meses**. **24)** Rotineiramente, esses registros **devem ser monitorados e analisados criticamente** observando principalmente: a) Tentativas frustradas de login; b) Acessos realizados; c) Violações de acesso;

ATIVIDADES	REGRAS/DIRETRIZES
	d) Acesso e Alteração nos registros de auditoria; e) Ações de administração (gestão de privilégios, alteração de políticas de senha, trocas de senha, deleção de usuários etc.), e; f) Manuseio de informações sensíveis.
REVISAR CONTAS E PERFIS	**25) As contas e acessos devem ser revisados ao menos trimestralmente pela Central de Serviços.** **26)** Durante essa revisão deve-se buscar, principalmente, por: a) Suspender contas inativas; b) Excluir usuários redundantes; c) Revogar acessos indevidos; d) Desabilitar perfis genéricos, padrão ou de fábrica; **27)** Os perfis devem ser revisados ao menos anualmente, visando que os perfis existentes estejam alinhados às necessidades do negócio. **28)** Essas revisões devem contar com participação dos Clientes.

7. PONTOS DE CONTROLE

7.1. INDICADORES DE DESEMPENHO (KPIS) DO SUBPROCESSO – GESTÃO DE SUPORTE DE TIC

Indicador	Satisfação de usuários com o atendimento de TI.
Descrição	Cada chamado registrado no sistema de chamados de TIC é passível de avaliação, que é feita em uma escala de 1 (muito ruim) até 5 (muito bom).
Periodicidade	Anual.
Polaridade	quanto maior, melhor.
Fonte	Sistema de Chamados – *Service Desk*.
Cálculo	$X = \left(\frac{\sum(atendimentos\ classificados\ em\ bom\ e\ muito\ bom)}{\sum(atendimentos)}\right) x\ 100\%$
Observações	Chamados sem nota de satisfação são encarados como classificados em "Muito Bom".

Indicador	Tempo médio para a resolução de um incidente.
Descrição	Apurar o tempo médio dispendido para a resolução de chamados no 1º e 2º nível técnico da Companhia.
Periodicidade	Mensal.
Polaridade	quanto menor, melhor.
Fonte	Sistema de Chamados – *Service Desk*.
Cálculo	$X = \left(\frac{\sum(tempo\ total\ em\ horas\ dispendido\ em\ resoluções\ de\ incidentes}{\sum(chamados\ resolvidos\ em\ 1º\ e\ 2º\ nível)}\right.$
Observações	*Σ (tempo total em horas dispendido em resolução de incidentes) =* soma do tempo dispendido pelo 1º e 2º nível em resoluções de incidentes *Σ (chamados resolvidos em 1º e 2º nível) =* quantidade total de chamados resolvidos em 1º e 2º nível. Para fins da somatória do tempo de que trata a fórmula, a contagem se inicia a partir do registro da requisição de serviço no Sistema de Chamados e é encerrada quando do encerramento do mencionado chamado.

7.2. INDICADORES DE DESEMPENHO (KPIS) DO SUBPROCESSO – GESTÃO DE INCIDENTES DE SI

Indicador	Quantidade de Eventos de SI&P.
Descrição	Identificar quantos chamados foram registrados como eventos de SI&P.
Periodicidade	Mensal.
Polaridade	quanto menor, melhor.
Fonte	Sistema de Chamados – *Service Desk*.
Cálculo	$X = \left(\sum Eventos\ de\ SI\&P\right)$
Observações	N/A

Indicador	Quantidade de Incidentes de SI&P.
Descrição	Identificar quantos chamados foram registrados como incidentes de SI&P.
Periodicidade	Mensal.
Polaridade	quanto menor, melhor.
Fonte	Sistema de Chamados – *Service Desk*.
Cálculo	$X = \left(\sum Incidentes\ de\ SI\&P\right)$
Observações	N/A

Indicador	Quantidade de Incidentes de SI envolvendo dados pessoais.
Descrição	Identificar quantos chamados foram registrados como incidentes de SI&P, que envolvam dados pessoais.
Periodicidade	Mensal.
Polaridade	quanto menor, melhor.
Fonte	Sistema de Chamados – *Service Desk*.
Cálculo	$X = \left(\sum Incidentes\ de\ SI\&P\ c/DP\right)$
Observações	N/A

7.3. INDICADORES DE DESEMPENHO (KPIS) DO SUBPROCESSO – GESTÃO DE NÍVEIS DE SERVIÇOS DE TIC

Indicador	Indicador geral de chamados resolvidos dentro do ANS.
Descrição	Aponta, dentro de todos os chamados técnicos atendidos e classificados dentro do CSTIC, a porcentagem de chamados que atendam o ANS

	acordado com todos os clientes dos Serviços de TIC oferecidos pela organização.
Periodicidade	Mensal.
Polaridade	Positiva.
Fonte	Relatório do Sistema de Gestão de chamados.
Cálculo	$X = \left(\frac{\sum(chamados\ que\ atenderam\ o\ SLA)}{\sum(chamados\ resolvidos)}\right) x\ 100\%$
Observações	*Σ(chamados resolvidos dentro do SLA) =* quantidade de chamados fechados no período que estão em conformidade com o Nível de Acordo de Serviço (ANS). *Σ(chamados resolvidos) =* quantidade total de chamados resolvidos.

Indicador	Indicador de cumprimento de ANS por cada Serviço de TIC.
Descrição	Aponta, dentro de todos os chamados técnicos atendidos e classificados dentro do CSTIC, a porcentagem de chamados que atenderam o ANS acordado com os Clientes dos Serviços de TIC oferecidos pela organização, segmentado por cada Serviço de TIC.
Periodicidade	Mensal.
Polaridade	Quanto maior, melhor.
Fonte	Relatório do Sistema de Gestão de chamados.
Cálculo	$X = \left(\frac{\sum(chamados\ que\ atenderam\ o\ SLA\ por\ cada\ serviço\ de\ TIC\ do\ CSTIC)}{\sum(chamados\ resolvidos\ por\ cada\ serviço\ de\ TIC\ do\ CSTIC)}\right)$
Observações	*Σ(chamados resolvidos dentro do SLA por cada serviço da TIC da CSTIC) =* quantidade de chamados fechados no período que estão em conformidade com o Nível de Acordo de Serviço (ANS). *Σ(chamados resolvidos por cada serviço da TIC da CSTIC) =* quantidade total de chamados resolvidos.

Indicador	Satisfação de Clientes e Usuários Chave com nível de Serviço.
Descrição	Avaliação de 1 (muito ruim) até 5 (muito bom), efetuada pelos clientes e usuários chave de cada serviço a respeito de sua satisfação com os níveis de serviços entregues. São considerados satisfeitos, aqueles que dão avaliação 4 (bom) ou 5 (muito bom).
Periodicidade	Anual.
Polaridade	Quanto maior, melhor.
Fonte	Pesquisa realizada junto ao público-alvo.
Cálculo	$X = \left(\frac{\sum(Usuários\ Chave\ ou\ Clientes\ satisfeitos)}{\sum(Usuários\ Chave\ ou\ Clientes)}\right) x\ 100\%$
Observações	*Para que o respondente tenha melhor embasamento na resposta, a pesquisa deve demonstrar as informações históricas de atendimento existentes como: chamados, satisfação dos usuários com atendimento, disponibilidade do serviço e cumprimento do ANS.*

7.4. INDICADORES DE DESEMPENHO (KPIS) DO SUBPROCESSO – GESTÃO DE ACESSOS LÓGICOS

Indicador	Nº de Incidentes envolvendo problemas de acesso.
Descrição	Aponta, dentro de todos os chamados fechados no período, quantos foram registrados como incidentes relacionados à problemas de acesso.
Periodicidade	Mensal.
Polaridade	Quanto menor, melhor.
Fonte	Sistema de Gestão de chamados.
Cálculo	$\mathrm{X}=(\sum(\text{Incidentes envolvendo problemas de acesso})$

Indicador	Tempo médio entre uma mudança e a atualização do acesso.
Descrição	Registro de tempo necessário para executar uma atualização de acesso de qualquer conta. O tempo deve ser contado a partir do momento em que o setor de TI recebe a notificação de que um acesso precisa ser atualizado, como e-mail do RH informando desligamento de um funcionário ou abertura de um chamado requisitando um novo acesso. A contagem se encerra assim que a alteração for executada.
Periodicidade	Mensal.
Polaridade	Quanto menor melhor.
Fonte	Sistema de Gestão de chamados ou Logs de administração de sistemas.
Cálculo	$X = \left(\frac{\sum(tempo\ de\ alteração\ de\ acesso)}{\sum(alterações\ de\ acesso\ realizadas)} \right) x\ 100\%$

Indicador	Nº de contas indevidas.
Descrição	Registra a quantidade de contas que se encontram em situação indevida. Entenda-se situação indevida acessos que não estão condizentes com o perfil/situação atual do usuário. Ex.: Funcionário do setor de Operações com acessos do setor de Meio Ambiente.
Periodicidade	Mensal.
Polaridade	Quanto menor melhor.
Fonte	Base de Quadro Funcional e Controle de Contas, Perfis e Acessos.
Cálculo	$\mathrm{X}=(\sum(\text{Contas com acesso indevido})$

8. PAPÉIS E RESPONSABILIDADES

8.1. SUPERVISÃO DE OPERAÇÃO E SOLUÇÕES DE TI (SEOTI)

<table>
<tr><th colspan="2">Responsável por</th></tr>
<tr><td colspan="2">

- Atuar como central de serviços;
- Manter a satisfação do cliente interno por meio do tratamento profissional e eficiente das requisições de serviço;
- Prover um canal para solicitação e recebimento de serviços padronizados para os quais exista um processo pré-definido de autorização e qualificação;
- Prover informação ao cliente interno sobre a disponibilidade de serviços e procedimentos para obtê-los;
- Prestar informações gerais e registrar dúvidas, comentários e reclamações.

</td></tr>
<tr><th>Principais atividades</th><th>Responsável por</th></tr>
<tr><td colspan="2">GESTÃO DE SUPORTE</td></tr>
<tr><td>TRIAGEM DE CHAMADO</td><td>

- Analisar e direcionar os chamados;
- Para os casos de incidentes de natureza grave, comunicar os gerentes de TI, para a adoção de medidas em caráter emergencial;
- Para eventos ou incidentes de SI&P comunicar imediatamente a ETIR.

</td></tr>
<tr><td>ATENDIMENTO DE CHAMADO</td><td>

- Prover suporte em 1º e 2º nível e escalonar para nível acima quando necessário;
- Acompanhar o ciclo de vida do chamado;
- Manter a base de conhecimento da Central de Serviços atualizada.

</td></tr>
<tr><td>CONCLUSÃO DE ATENDIMENTO DE CHAMADO</td><td>

- Elaborar diagnóstico da resolução ou laudo técnico do chamado.

</td></tr>
<tr><td>MONITORAMENTO</td><td>

- Mensurar e monitorar os indicadores de desempenho na periodicidade definidos neste normativo;
- Emitir relatórios mensais e encaminhar ao Comitê de TI.

</td></tr>
<tr><td>GERENCIAMENTO DE PROBLEMAS</td><td>

- Identificar problemas e aplicar, em conjunto com as áreas de TI, solução de contorno ou, quando possível, correção definitiva.

</td></tr>
<tr><td colspan="2">GESTÃO DE NÍVEIS DE SERVIÇO DE TIC</td></tr>
<tr><td colspan="2">

- Conduzir o processo de Formalização de Índices de ANS e ANO junto aos Clientes de Serviço de TIC e às Áreas de Negócio de TIC.

</td></tr>
</table>

DETERMINAÇÃO DAS INFORMAÇÕES DO ANS	• Fornecer informações pertinentes ao suporte e operações de TIC; • Conduzir e auxiliar no fornecimento das demais informações advindas das áreas de negócio e de TIC.
FORMALIZAÇÃO DO ANS	• Viabilizar a formalização do ANS por meio de negociações e mediações entre áreas de negócio e de TIC.
MONITORAMENTO E REVISÃO DOS ANS	• Realizar o monitoramento do atendimento dos níveis de serviço e das avaliações dos clientes e usuários; • Emitir e divulgar relatórios de desempenho dos ANSs.
GESTÃO DE ACESSOS LÓGICOS	
• Manter o inventário de contas; • Definir os perfis e revisá-los periodicamente com apoio do negócio; • Atender as requisições de acessou ou atualização de acesso; • Analisar as requisições de Acesso; • Efetuar a liberação e remoção de acessos, e; • Monitorar as atividades das contas.	

8.2. USUÁRIO REQUISITANTE/EMPREGADO DA COMPANHIA

Principais atividades	Responsável por
GESTÃO DE SUPORTE	
ABERTURA DE CHAMADO	• Registrar chamado no Sistema de Gestão de Serviços de TIC.
CONCLUSÃO DE ATENDIMENTO DE CHAMADO	• Concluir o chamado no prazo estabelecido após a solução do atendimento pela área de TI; • Responder à pesquisa de satisfação do atendimento.
GESTÃO DE INCIDENTES DE SI&P	
MONITORAMENTO E IDENTIFICAÇÃO DE EVENTOS DE SI&P	• Reportar imediatamente qualquer evento/incidente de SI&P que presenciar; • Como gestor ou fiscal de contratos com compartilhamento de informações da APS: Receber comunicação de incidentes de SI&P ou violação de dados pessoais por parte de agentes de tratamento (fornecedores) que estejam sob a sua responsabilidade; • Não deve tentar provar as suspeitas de fragilidades de segurança da informação. Testar fraquezas podem ser

	encaradas como mau uso e podem causar danos aos serviços de TIC. Podendo o mesmo ser punido por isso.
TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VALIDAÇÃO	• Auxiliar nos processos de investigação do incidente.
GESTÃO DE NÍVEIS DE SERVIÇO DE TIC	
• No papel de cliente de serviços de TIC, é a pessoa responsável por negociar índices de ANS com as Áreas de Negócio de TIC, representando os usuários de Serviços de TIC.	
GESTÃO DE ACESSOS LÓGICOS	
• Solicitar alterações de acesso conforme sua necessidade; • Fornecer informações necessárias para que a central de serviços efetue a gestão dos acessos; • Informar quando identificar que tem acesso a qualquer informação que não seja adequada ao seu perfil. De modo que a Central de Serviços possa corrigir o problema.	

8.3. COORDENADOR DA ETIR

Responsável por	
• Liderar e tomar decisões sobre à resposta a incidentes de segurança da informação. • Buscar a disponibilização de recursos necessários para a efetiva gestão de incidentes de segurança da informação; • Revisar e aprovar planos de resposta a incidentes e supervisionar sua a implementação; • Revisar e criticar os planos de resposta a incidentes; • Coordenar internamente e externamente a ETIR em ações preventivas ou reativas de incidentes de SI&P; • Assumir as mesmas responsabilidades descritas para o papel de membro da ETIR.	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	
PLANEJAMENTO - PREVENÇÃO DE INCIDENTES DE SI&P	• Pautar e coordenar a reunião periódica da ETIR; • Com o apoio dos demais membros da ETIR, preparar material para auxiliar a tomada de decisões para a prevenção dos incidentes de SI&P.
TRATAMENTO DE INCIDENTES DE	• Reunir a ETIR e quem mais for necessário na Sala de Crise (War Room).

SI&P – PLANEJAMENTO	• Centralizar as informações para fornecê-las às partes interessadas; • Controlar o acesso à Gerência de Infraestrutura de Dados.
COLETA E MANUSEIO DE EVIDÊNCIAS FORENSES	• Providenciar as evidências necessárias para apuração e responsabilização de condutas ilícitas; • preencher Termo de Custódia dos Ativos de Informação relacionados ao Incidente de SI&P
COMUNICAÇÃO ÀS AUTORIDADES POLÍCIAIS COMPETENTES	• Acionar o Presidente da Companhia sobre a necessidade de comunicar às autoridades competentes.

8.4. ETIR

Responsável por	
• Facilitar e a coordenar as atividades de tratamento e resposta a incidentes de SI&P; • Tratar artefatos maliciosos; • Tratar vulnerabilidades; • Emitir alertas, advertências e anúncios de ocorrência de incidentes de SI&P; • Emitir anúncios; • Prospectar ou monitorar novas tecnologias de segurança cibernética; • Avaliar a segurança do ambiente computacional; • Detectar intrusões.	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	
PLANEJAMENTO - PREVENÇÃO DE INCIDENTES DE SI&P	• Desenvolver, implementar e manter procedimentos para preparar e planejar a resposta a incidentes de SI&P; • Preparar material para auxiliar a tomada de decisões para a prevenção dos incidentes de SI&P.
MONITORAMENTO E IDENTIFICAÇÃO DE EVENTOS DE SI&P	• Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando identificar eventos que possam causar impacto na disponibilidade, integridade e confidencialidade de dados pessoais que sejam tratados pela Companhia; • Identificar e notificar eventos ou incidentes de SI&P; • Executar ou acompanhar as atualizações de segurança.
IDENTIFICAÇÃO DE INCIDENTES DE SI&P	• Avaliar e decidir se um evento de SI&P é caracterizado ou não como incidente de SI&P e se envolve ou não dados pessoais; • Comunicar o ETPD em caso de violação de dados pessoais.

TRATAMENTO DE INCIDENTES DE SI&P – PLANEJAMENTO	• Participar da reunião de planejamento em sala de crise, caso convocado.
TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VISTORIA	• Responder e vistoriar o incidente; • Auxiliar nos processos de investigação do incidente quando requerido; • Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente.
REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P	• Documentar o tratamento do incidente de SI&P.
GESTÃO DE ACESSOS LÓGICOS	
• Consultar os resultados dos monitoramentos das atividades de contas de usuários a fim de identificar incidentes de SI&P.	

8.5. ETPD

Responsável por	
• **Tratar os incidentes de violação de dados pessoais**	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	
PLANEJAMENTO - PREVENÇÃO DE INCIDENTES DE SI&P	• Propor medidas de prevenção à incidentes de violação de dados pessoais.
IDENTIFICAÇÃO DO INCIDENTE DE SI&P	• Confirmar potenciais incidentes de violação de dados pessoais; Envolver áreas correlatas para análise do potencial incidente.
TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VISTORIA	• Orientar: o tratamento da violação de dados pessoais; o comunicação violação de dados pessoais; o avaliação de riscos de violação de dados pessoais; o afetados pela violação de dados pessoais sobre medidas corretivas a serem tomadas;

AVALIAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS	Apoiar a avaliação de riscos oriundos da violação de dados pessoais.
REGISTRO DO GERENCIAMENTO DE EVENTOS E INCIDENTES DE SI&P	• Registrar as atividades de tratamento de violação de dados pessoais.
COMUNICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS	• Coordenar a comunicação, à ANPD, titulares dos dados pessoais e aos controladores, quando couber.
GESTÃO DE ACESSOS LÓGICOS	
• Consultar os resultados dos monitoramentos das atividades de contas de usuários a fim de identificar incidentes de SI&P que envolvam dados pessoais.	

8.6. GESTOR DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Responsável por	
• Tomar decisões que extrapolem a autonomia do coordenador da ETIR; • Supervisionar as ações da ETIR e de seu coordenador; • Aprovar e empreender ações investimentos que promovam a melhoria contínua da gestão de incidentes de SI&P; • Fomentar o patrocínio da alta administração e apoio das áreas de negócio aos assuntos ligados à Incidentes de SI&P.	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	
PLANEJAMENTO - PREVENÇÃO DE INCIDENTES DE SI&P	• Participar da reunião periódica de prevenção de incidentes de SI&P.
TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VISTORIA	• Realizar interface da ETIR com as partes interessadas no incidente de SI&P: Alta administração, áreas de negócio, entes externos e órgãos de controle etc; • Resolver conflitos a fim de prover um atendimento mais rápido ao incidente de SI&P.

8.7. SUPERINTENDÊNCIA JURÍDICA (SUJUD)

Responsável por	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	
COLETA E MANUSEIO DE EVIDÊNCIAS FORENSES	• Identificar as consequências legais do incidente de SI&P e quais autoridades devem ser comunicadas.
COMUNICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS	• Apoio ao comunicado aos titulares dos dados pessoais.

8.8. SUPERINTENDÊNCIA DE COMUNICAÇÃO CORPORATIVA (SUCOC)

Responsável por	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	
TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VISTORIA	• No caso de incidentes que tiverem desdobramentos para fora da Companhia e que envolvam a imprensa ou comunidade externa, prestar suporte na elaboração do plano de comunicação aos titulares de dados e pessoas envolvidas no incidente.
COMUNICAÇÃO DE VIOLAÇÃO DE DADOS PESSOAIS	• Apoio ao comunicado aos titulares dos dados pessoais.

8.9. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (CSI)

Responsável por	
• Tomar decisões sobre plano de comunicação aos titulares de dados; • Tomar decisões sobre plano de comunicação aos clientes e ao mercado.	
Principais atividades	**Responsável por**
GESTÃO DE INCIDENTES DE SI&P	

TRATAMENTO DE INCIDENTES DE SI&P – RESPOSTA E VISTORIA	• Resolver conflitos a fim de prover um atendimento mais rápido ao incidente de SI&P.

8.10. ÁREAS DE NEGÓCIO DE TIC (GERID e GEDES)

Principais atividades	Responsável por
GESTÃO DE NÍVEIS DE SERVIÇO DE TIC	
• Receber os dados da Central de Serviços, avaliando-os e propondo novos índices de ANS para os Clientes de Serviço de TIC.	
GESTÃO DE ACESSOS LÓGICOS	
MONITORAR ATIVIDADES DAS CONTAS	• Habilitar e fornecer condições para o registro de logs/eventos dos sistemas.

9. DISPOSIÇÕES FINAIS

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

10. ANEXOS

ANEXO I - FORMULÁRIO DE ANS

CELEBRAÇÃO DE ANS

PORTO DE SANTOS AUTORIDADE PORTUÁRIA SEOTI - SUPERVISÃO DE OPERAÇÃO E SOLUÇÕES DE TI

ANS – Celebração de Acordo de Nível de Serviços de TI	Nº 01/2022
Nome Curto do Serviço:	Vigência a partir de:

Partes Envolvidas	
Cliente *(Preenchimento: Fornecedor do Serviço)*	*Orientação para Preenchimento deste campo:* *Nome do Cliente de Serviço de TIC.*
Área de Negócio *(Preenchimento: Cliente do Serviço)*	*Orientação para Preenchimento deste campo:* *Nome da Área de Negócio atendida.*
Responsabilidades da Área de Negócio *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor e a SEOTI)*	*Orientação para Preenchimento deste campo:* *Relacionar todas as responsabilidades e atividades da Área de Negócio em relação ao Serviço aqui descrito, como por exemplo, fatores como administração de usuários, atendimento e resolução de dúvidas quanto à utilização do Serviço, monitoramento de disponibilidade e desempenho, notificação e alerta de eventuais falhas recorrentes ou catastróficas, dentre outros, assim como a notificação e requisição de mudanças necessárias ao Serviço, que possam exigir uma revisão do SLA.*
Provedor *(Preenchimento: Provedor)*	*Orientação para Preenchimento deste campo:* *Nome do Analista de TIC responsável pela concepção do Serviço de TIC.*
Área de TIC *(Preenchimento: Provedor)*	*Orientação para Preenchimento deste campo:* *Área de TIC responsável pela concepção do Serviço de TIC.*
Responsabilidades da Área de TIC *(Preenchimento: Fornecedor do Serviço)*	*Orientação para Preenchimento deste campo:* *Relacionar todas as responsabilidades e atividades da Área de TIC em relação ao Serviço aqui descrito, como por exemplo, fatores como a manutenção, operação, sustentação, suporte, e demais atividades envolvidas no atingimento dos níveis de serviços acordados.*

Serviço			
Nome *(Preenchimento: SEOTI)*	*Orientação para Preenchimento deste campo:* *Nome do Serviço de TIC.*	**Número** *(Preenchimento: SEOTI)*	
Contexto *(Preenchimento: SEOTI)*	*Orientação para Preenchimento deste campo:* *Definição do processo de negócio coberto pelo serviço de forma detalhada.*		
Escopo *(Preenchimento: SEOTI, em conjunto com o Cliente e o Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *O que se inclui e o que se exclui deste acordo.*		

Resultados Esperados	
Funcionalidade *(Preenchimento: Cliente, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *O Analista propõe uma descrição das funções mínimas e essenciais deste Novo Serviço de TIC, determinadas a partir dos requisitos resultantes da análise do DOD, para que o Cliente de TIC possa concordar com este escopo de funcionalidades.*
Confiabilidade *(Preenchimento: Cliente, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *O Analista deverá propor um número máximo de quedas que podem ser toleradas dentro de um período determinado. Podem ser quedas gerais do Serviço de TIC, ou quedas por funcionalidade/grupo de funcionalidades / funções de sistema, ou outras partes ou trechos do Novo Serviço de TIC. Poderá haver também diferentes confiabilidades por Setor ou Localidade. Por exemplo: 4 quedas por dia, 2 quedas por semana etc.*
Disponibilidade *(Preenchimento: Cliente, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *Caso não conste do DOD, o Analista deverá entrevistar o Cliente de TIC a respeito dos horários em que o Serviço deverá estar disponível (inclusive dias da semana, feriados e horários críticos/horas de menor demanda e prioridade, datas de fechamento de relatório/fechamento de mês/datas-limite por força de legislação ou norma técnica).*

Segurança	
Registros de Auditoria *(Preenchimento: Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *Listar abaixo as ações de gestão de logs, se houverem, com as ações de registro de "Acesso Concedido" e "Acesso Negado", devendo os registros serem armazenados por, no mínimo, 3 meses, com data e hora de cada ocorrência. Descrever com mais detalhes na Tabela do Anexo I.*
Perfis de Acesso *(Preenchimento: Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *Listar abaixo os perfis de acesso de usuário disponíveis no Serviço de TIC, e descrever com mais detalhes na Tabela do Anexo I.*
Regramentos de SI&P *(Preenchimento: Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *Preencha as previsões de SI&P deste Serviço. As normas mínimas de SI&P da SPA estão no Anexo II.*

Padrões e Procedimentos	
Procedimentos para requisição de serviços *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento deste campo:* *O Analista deverá explicar quais operações do sistema serão classificadas como Ocorrências para Requisição de Serviços dentro do Novo Serviço de TIC, para a aprovação do Cliente de TIC. Também deverá entrar em acordo com o Cliente sobre as formas de contato admissíveis com quem atenderia cada Requisição de Serviço (pois algumas Requisições de Serviço podem não ser feitas pelo Sistema de Chamados de TIC, por exemplo), os horários em que as Requisições de Serviço poderão ser atendidas, e o que fazer fora desse horário para demandar ou solicitar a realização imediata da Requisição de Serviço (ou se nem mesmo este serviço fora de horário estará disponível). Também devem ser explicadas as Mudanças Padrão que devem ser tratadas como chamados de Requisição de Serviços.*

Procedimentos de escalação *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento desse campo:* *O Analista deverá entrevistar o Cliente de TIC para determinar se existirão Procedimentos de Escalação para este Novo Serviço de TIC, contando com os detalhes dos contatos dentro de cada uma das partes envolvidas no acordo e os processos de encaminhamento e pontos de contato, caso seja necessário.*
Procedimentos de mudança *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento desse campo:* *Breve menção e/ou referência aos procedimentos de gerenciamento de mudanças, tratamento e implementação destas).*
Definições e situações de emergência *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor do Serviço)*	*Orientação para Preenchimento desse campo:* *O Analista deverá entrevistar o Cliente de TIC para determinar se existirão Procedimentos e Situações de Emergência para este Novo Serviço de TIC, contando com os detalhes dos contatos dentro de cada uma das partes envolvidas no acordo e os processos de encaminhamento e pontos de contato, caso seja necessário, conjugados com os Procedimentos de Gestão de Continuidade, caso existam.*

PORTO DE SANTOS AUTORIDADE PORTUÁRIA SEOTI - SUPERVISÃO DE OPERAÇÃO E SOLUÇÕES DE TI

Itens do CSTIC a serem incluídos		ANS
Descrição do Cadastro da Categoria/Item de Serviço no CSTIC *Orientação:* *Deve ser preenchido 01 (um) item para INCIDENTES e 01 (um) item para REQUISIÇÕES, porém exceções podem ser feitas.*		
Tipo de Ocorrência *(Preenchimento: SEOTI, em conjunto com o Provedor)*	*Orientação:* *Selecione "Incidente" para o cadastro de uma falha, defeito ou interrupção não planejada de um serviço de TI ou, ainda, a redução da qualidade/velocidade ou dificuldade de acesso desse serviço.* *Selecione "Requisição" para o cadastro de solicitação de serviço é um pedido do cliente por informações ou recomendações, ou por uma alteração de um padrão (uma mudança pré-aprovada que tem baixo risco, é relativamente comum e dá continuidade a um procedimento), ou para obter acesso a um serviço de TI.* **Incidente - ☐** **Requisição - ☐**	
Nome da Categoria *(Preenchimento: SEOTI, em conjunto com o Provedor)*	*Orientação:* *Nome por extenso, de acordo com o padrão do CSTIC (pode ser uma Categoria já existente).*	
Nome do Item de Serviço *(Preenchimento: SEOTI, em conjunto com o Provedor)*	*Orientação:* *Nome por extenso, de acordo com o padrão do CSTIC (pode ser um item de Serviço já existente, caso seja uma atualização de acordo). Pode ser deixado em branco para "Incidentes genéricos".*	
ANS Acordado *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor e a SEOTI)*	**Índice de ANS Anterior** ***(Preenchimento: SEOTI)***	**Novo Índice de ANS** ***(Preenchimento: Cliente)***
	Consultar GLPI e ANS anterior para preencher. Preencher antes de entregar ao usuário (em branco se "Novo Serviço").	*Tempo para atendimento em horas inteiras*
Descrição do Cadastro da Categoria/Item de Serviço no CSTIC		
Tipo de Ocorrência *(Preenchimento: SEOTI, em conjunto com o Provedor)*	*Orientação:* *Selecione "Incidente" para o cadastro de uma falha, defeito ou interrupção não planejada de um serviço de TI ou, ainda, a redução da qualidade/velocidade ou dificuldade de acesso desse serviço.* *Selecione "Requisição" para o cadastro de solicitação de serviço é um pedido do cliente por informações ou recomendações, ou por uma alteração de um padrão (uma mudança pré-aprovada que tem baixo risco, é relativamente comum e dá continuidade a um procedimento), ou para obter acesso a um serviço de TI.* **Incidente - ☐** **Requisição - ☐**	
Nome da Categoria *(Preenchimento: SEOTI, em conjunto com o Provedor)*	*Orientação:* *Nome por extenso, de acordo com o padrão do CSTIC (pode ser uma Categoria já existente).*	
Nome do Item de Serviço *(Preenchimento: SEOTI, em conjunto com o Provedor)*	*Orientação:* *Nome por extenso, de acordo com o padrão do CSTIC (pode ser um item de Serviço já existente, caso seja uma atualização de acordo). Pode ser deixado em branco para "Incidentes genéricos".*	
ANS Acordado *(Preenchimento: Cliente do Serviço, em conjunto com o Provedor e a SEOTI)*	**Índice de ANS Anterior** ***(Preenchimento: SEOTI)***	**Novo Índice de ANS** ***(Preenchimento: Cliente)***
	Consultar GLPI e ANS anterior para preencher. Preencher antes de entregar ao usuário (em branco se "Novo Serviço").	*Tempo para atendimento em horas inteiras.*

PORTO DE SANTOS AUTORIDADE PORTUÁRIA

ANEXO I – PERFIS DE ACESSO

(Preenchimento: Provedor)

PERFIL	DIREITOS	PERMISSOES	ITEM DO SERVIÇO
<Perfil 1>			
<Perfil 2>			
<Perfil 3>			

PORTO DE SANTOS

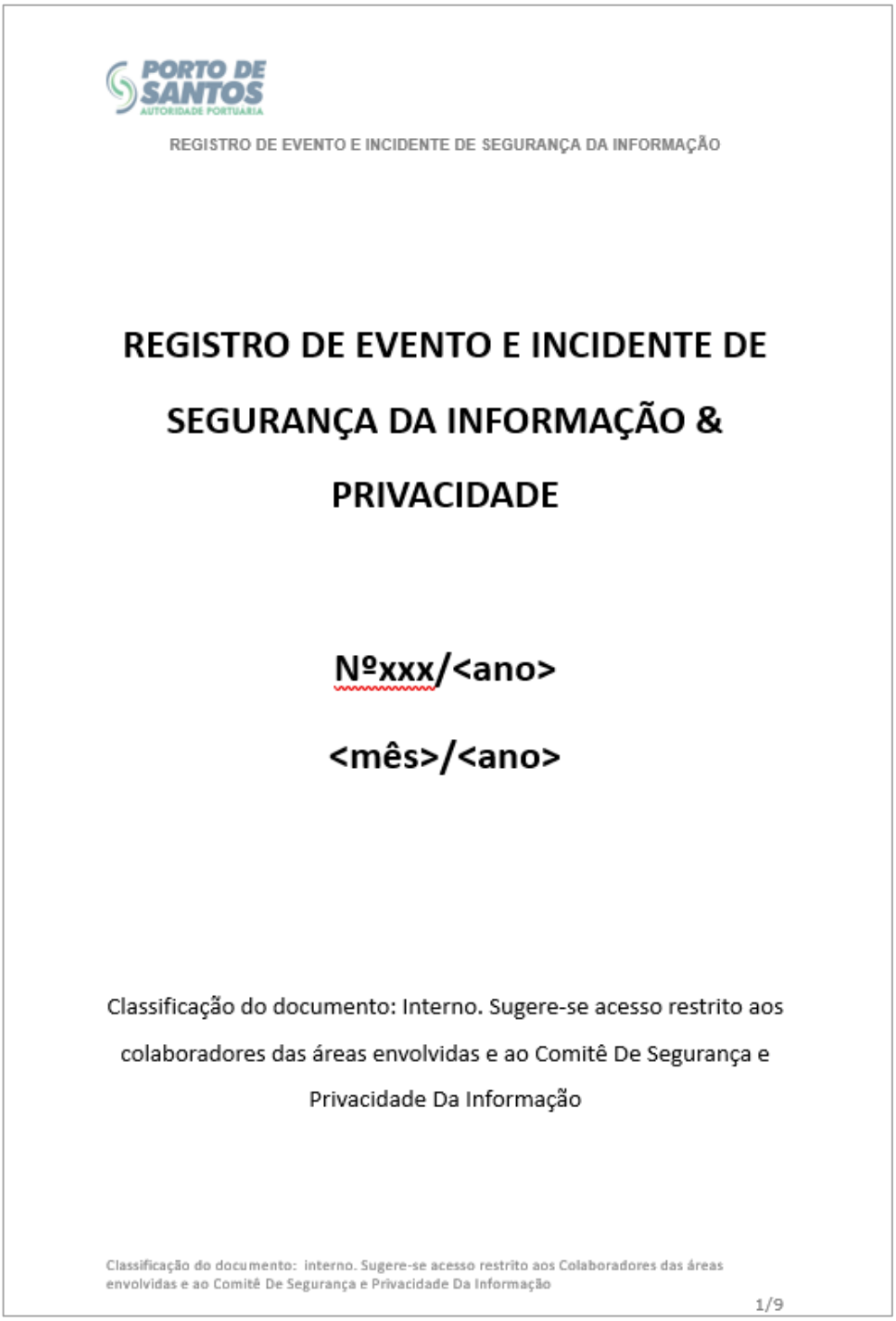
ANEXO II – NORMAS DE SI&P

(Preenchimento: Proponente)

O Arrendatário deve consultar as Políticas de Segurança vigentes com a Área Responsável, e apresentar os requerimentos exibidos ao Cliente de TIC, para que ele possa concordar com as ações propostas, além das ações que o próprio Cliente possa ter incluído no DOD.

NORMA SGPI	RELAÇÃO COM O SERVIÇO	SEGUIR?
POLÍTICA DE SEGURANÇA	• Classificação da Informação	✓
GESTÃO DE PESSOAS	• Desativar acesso ao desligamento do empregado	✓
GESTÃO DE ACESSOS	• Manutenção de contas de acesso • Nível mínimo de senha	✓
CRIPTOGRAFIA	• Chaves criptográficas para acesso à informação	✓
SEGURANÇA FISICA E AMBIENTE	• Restrição de acesso físico às instalações. Definição de Perímetro	⛔
INCIDENTES DE SI E VIOLAÇÃO DE DP	• Registro de incidentes de segurança	✓
PRIVACIDADE POR DESENHO E POR PADRÃO	• Prevalecer a privacidade em relação ao serviço quando houver situação de dúvida;	✓
SI EM CONTINUIDADE DE NEGÓCIO	• Plano de contingência, recuperação etc.	✓
PROCESSO DE SOFTWARE	• Manutenção de ambiente de teste segregado do de produção, dados pessoais pseudonimizados	✓

ANEXO II - REGISTRO DE EVENTO E INCIDENTE DE SEGURANÇA DA INFORMAÇÃO



PORTO DE SANTOS
AUTORIDADE PORTUÁRIA

REGISTRO DE EVENTO E INCIDENTE DE SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE

Nºxxx/<ano>

<mês>/<ano>

Classificação do documento: Interno. Sugere-se acesso restrito aos colaboradores das áreas envolvidas e ao Comitê De Segurança e Privacidade Da Informação

Sumário

REGISTRO DE EVENTO E INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

1. INFORMAÇÕES DE CONTROLE E CONTATO	
1.1. REGISTRO NÚMERO	
1.2. COORDENADOR DA ETIR	
1.3. EMAIL COORDENADOR ETIR	
1.4. TELEFONE COORDENADOR DA ETIR	
1.5. RESPONSÁVEL PELA PRESERVAÇÃO DOS DADOS DO INCIDENTE	
1.6. TELEFONE DO RESPOONSÁVEL	
2. CLASSIFICAÇÃO (EVENTO/INCIDENTE):	
3. CRITICIDADE/IMPACTO (VIDE TABELA)	
4. PRIORIDADE (VIDE MATRIZ PRIORIZAÇÃO)	

TABELA DE CRITICIDADE

CENÁRIOS	PILAR DE SI COMPROMETIDO			CRITICIDADE
	C	I	D	
Cenário 1	SIM	SIM	SIM	ALTA
Cenário 2	SIM	SIM	NÃO	ALTA
Cenário 3	NÃO	SIM	SIM	ALTA
Cenário 4	SIM	NÃO	SIM	ALTA
Cenário 5	SIM	NÃO	NÃO	ALTA
Cenário 6	NÃO	SIM	NÃO	MÉDIA
Cenário 7	NÃO	NÃO	SIM	BAIXA

MATRIZ DE PRIORIZAÇÃO

		CRITICIDADE		
		BAIXA	MÉDIA	ALTA
IMPACTO	BAIXO	BAIXA	BAIXA	MÉDIA
	MÉDIO	BAIXA	MEDIO	ALTA
	ALTO	MÉDIA	ALTA	ALTA

Impacto:

Baixa: afeta um grupo pequeno de usuários.

Média: afeta um departamento inteiro.

Alta: afeta uma região inteira

5. INFORMAÇÕES SOBRE O INCIDENTE

Classificação do documento: interno. Sugere-se acesso restrito aos Colaboradores das áreas envolvidas e ao Comitê De Segurança e Privacidade Da Informação

4/9

5.1. ESCALAÇÃO DO EVENTO PARA INCIDENTE
5.2. DATA DA IDENTIFICAÇÃO
5.3. DESCRIÇÃO
5.4. SETOR ONDE OCORREU
5.5. COMO FOI DETECTADO
5.6. IDENTIFICAÇÃO DE QUEM REPORTOU
5.7. EQUIPE DE RESPOSTA
5.8. DATA DO EVENTO/DATA DE IDENTIFICAÇÃO
5.9. DATA/HORA PREVISTA DA SOLUÇÃO
5.10.DATA/HORA SOLUÇÃO
5.11.LISTA DE COMUNICAÇÃO (PESSOAS, ETC)
5.12.ENVOLVE DADOS PESSOAIS (Sim/Não):
6. DIAGNOSTICO E TRATAMENTO
6.1. NATUREZA DO EVENTO
6.2. CAUSA RAIZ IDENTIFICADA
6.3. ATIVOS AFETADOS
6.4. IMPACTO
6.5. PROVIDENCIAS TOMADAS PARA INVESTIGAÇÃO E SETORES ENVOLVIDOS
6.6. RESULTADO DA INVESTIGAÇÃO

PORTO DE SANTOS
AUTORIDADE PORTUARIA

REGISTRO DE EVENTO E INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

6.7. DELIBERAÇÃO PARA AS AÇÕES DE CONTORNO E SOLUÇÃO APLICÁVEIS
6.8. CAUSA RAIZ RESOLVIDA
7. EVIDÊNCIAS
7.1. DADOS COLETADOSR PRESERVADOS E OUTROS DADOS RELEVANTES
7.2. TERMO DE CUSTÓDIA DOS ATIVOS DE INFORMAÇÃO RELACIONADIS AO INCIDENTES DE SEGURANÇA
7.3. NÚMERO DE LACRE DE MATERIAL FÍSICO PRESERVADO, SE HOUVER
7.4. JUSTIFICATIVA SOBRE A INVIABILIDADE DE PRESERVAÇÃO DE MÍDIAS DE ARMAZENAMENTO DOS DISPOSITIVOS AFETADOS
8. VIOLAÇÃO DE DADOS PESSOAIS:
8.1. NATUREZA DOS DADOS PESSOAIS VIOLADOS
8.2. TITULARES ENVOLVIDOS
8.3. MEDIDAS TECNICAS E DE SEGURNÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS
8.4. RISCOS RELACIONADOS AO INCIDENTE
8.5. JUSTIIFCATIVA DE REGISTRO E COMUNICAÇÃO TARDIA
8.6. MEDIDAS QUE FORAM /SERÃO ADOTADAS PARA MITIGAR EFEITOS DO INCIDENTE
8.7. PONTOS DE CONTATO PARA MELHORES DETALHES
8.8. POSSIVIES CONSEQUENCIAS DO INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS
8.9. CONCLUSÃO SOBRE DADOS PESSOAIS DO EVENTO
9. OUTRAS INFORMAÇÕES RELEVANTES

Classificação do documento: interno. Sugere-se acesso restrito aos Colaboradores das áreas envolvidas e ao Comitê De Segurança e Privacidade Da Informação

6/9

REGISTRO DE EVENTO E INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

10. CONCLUSÃO

ANEXO I –

ANEXO II –