MANUAL SGPI - SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE (SI&P)

Sumário

MANUAL SGPI – SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE (SI&P)

1. DISPOSIÇÕES INICIAIS

Fica instituído o Manual SGPI - Segurança da Informação & Privacidade (SI&P) da Autoridade Portuária de Santos S.A. (“Companhia”) como parte integrante do conjunto de instrumentos de governança e de gestão que suportam a concepção, implementação e melhoria contínua na estrutura organizacional da Companhia.

2. INTRODUÇÃO

Este Manual é parte integrante do Sistema de Gestão da Segurança da Informação e Privacidade (SGPI) e busca abordar todos os assuntos pertinentes com segurança da informação e privacidade no âmbito da Companhia.

3. DEFINIÇÕES

Para os fins deste Manual são adotados os seguintes conceitos:

Acesso de Administradores: Acesso efetuado a ativos de Tecnologia da Informação (TI) com direitos de Administração sobre o ativo. Direito de administrador tem total poder sobre o funcionamento do ativo de TI.

Acordo de Nível de Serviço (ANS): Acordo firmado entre a área de TI e as áreas de negócios da Companhia que utilizam os serviços de TI. Este acordo descreve os serviços de TI, suas metas de nível de serviço, além dos papéis e responsabilidades das partes envolvidas no acordo.

Anonimização: Técnica que através da “utilização de métodos técnicos razoáveis e disponíveis no momento do tratamento dos dados, faz com que uma informação perca a capacidade de associação, direta ou indireta, a um indivíduo” e que resulte em dado anonimizado (dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento).

Áreas Seguras de TI: Espaços físicos que precisam de proteção contra as ameaças, que poderiam gerar um incidente de segurança da informação.

Arquivos Temporários: Arquivos criados como resultado de tratamento de dados pessoais, específicos de um sistema ou aplicação ou banco de dados (inclusive para *rollback* de transações).

Avaliação de impactos à privacidade: Processo que permite identificar e avaliar os impactos e riscos à privacidade do titular associados ao processamento de Dados pessoais. O documento resultante contém a descrição dos processos de tratamento de dados pessoais com as medidas, salvaguardas e mecanismos de mitigação de risco. Serve de base para elaboração do RIPD. Esta avaliação de riscos é focada no titular e não na empresa e seus ativos como nos riscos corporativos e riscos de segurança da informação e privacidade.

Avaliação de Legítimo Interesse: Processo para identificar se fatores que caracterizam o legítimo interesse estão presentes na atividade e assim confirmar a possibilidade de utilizar a Hipótese Legal Legítimo Interesse. O legítimo interesse é uma das bases legais para o processamento de dados pessoais, desde que seja necessário para os interesses legítimos da organização ou de um terceiro, a menos que esses interesses sejam anulados pelos interesses ou direitos e liberdades fundamentais do titular dos dados.

Ativo de Informação: Qualquer componente (tecnológico, software etc.) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio e que tem valor para a empresa. Os ativos reunidos em um inventário nesse contexto, não tem relação com um inventário de hardware e software.

Certificado Digital: Assinatura digital que garante agilidade e segurança nas transações eletrônica de dados.

Chave privada: Também chamada de criptografia de chave simétrica, secreta ou única, utiliza uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para garantir a confidencialidade dos dados.

Chave pública: Criptografia de chave pública, também conhecida como criptografia assimétrica, é qualquer sistema criptográfico que usa pares de chaves: chaves públicas, que

podem ser amplamente disseminadas. Em um sistema de criptografia de chave pública, qualquer pessoa pode criptografar uma mensagem usando a chave pública do destinatário.

Código de ética da EC-Council: Código de ética utilizado como parâmetro por profissionais especializados na atividade de "hackeamento" ético, composto dos seguintes itens:

i. Manter a confidencialidade das informações obtidas durante os testes, não podendo vender ou repassar sem a permissão por escrito do cliente;
ii. Proteger a propriedade intelectual dos outros;
iii. Divulgar às pessoas apropriadas ou autoridades, os perigos de qualquer cliente de e-commerce, da comunidade da internet ou de qualquer pessoa relacionada a uma transação eletrônica via software ou hardware;
iv. Prover um serviço com qualidade dentro da sua área de conhecimento e sendo honesto quanto a sua capacidade técnica;
v. Nunca usar um software obtido de forma ilegal ou antiética;
vi. Não se envolver em práticas financeiras fraudulentas como suborno, dupla cobrança ou práticas financeiras inadequadas;
vii. Usar as informações do cliente ou empregador de forma consciente e somente o que foi autorizado;
viii. Ter uma conduta de forma ética e competente o tempo inteiro;
ix. Não ter envolvimento com hackers ou atividades maliciosas;
x. Não comprometer de forma proposital os sistemas dos clientes durante sua atividade profissional;
xi. Garantir que todos os *pentests* sejam autorizados e dentro da legalidade;
xii. Não violar nenhuma lei.

Compartilhamento de Dados: Disponibilização de dados pelo gestor para determinado recebedor de dados (fonte: Decreto 10.046/2019, Art. 2º item VIII). O mesmo conceito pode ser adotado quando os dados são pessoais.

Computação em Nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos

computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem (PSN).

Controlador: Art. 5º, VI, da LGPD: Pessoa Jurídica ou Física de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Não são controladoras as pessoas naturais que atuam como profissionais subordinados a uma pessoa jurídica ou como membros de seus órgãos.

Controladoria conjunta: Determinação conjunta, comum ou convergente, por dois ou mais controladores, das finalidades e dos elementos essenciais para a realização do tratamento de dados pessoais, por meio de acordo que estabeleça as respectivas responsabilidades quanto ao cumprimento da LGPD (Fonte: Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado de maio/2021 item 46).

CPADS: Comissão de Permanente de Avaliação de Documentos Sigilosos.

Criptografia: Procedimento para garantir, através de codificação do próprio dado, que apenas quem tiver conhecimento do mecanismo de descodificação, terá acesso ao mesmo.

Cookie: Um pequeno arquivo que é salvo no computador das pessoas para ajudar a armazenar informações usadas na navegação nas páginas da Web visitadas pelo usuário. Este componente dos dados de navegação, dependendo das informações armazenadas pode caracterizar um tratamento de dados pessoais.

Declaração de Aplicabilidade: Documento resultante de uma avaliação de Riscos de Segurança e Privacidade, onde se encontram os controles (baseados nas normas ISO 27701/27001/27002), aplicáveis para mitigação de riscos de Segurança da Informação e Privacidade (SI&P), também conhecido como SoA do inglês “Statement of Aplicability”.

Divulgação: Ato, processo ou efeito de divulgar, de tornar alguma coisa pública; difusão, propagação, publicidade.

DPO (Data Protection Officer) ou encarregado pelo Tratamento de Dados Pessoais: é o profissional responsável por garantir que a companhia cumpra as normas de proteção de dados pessoais.

EC-Council: Conselho Internacional de Consultores de Comércio Eletrônico. É uma organização americana que oferece certificação, educação, treinamento e serviços em segurança cibernética em várias habilidades de segurança cibernética.

Encarregado pelo Tratamento de Dados: Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados – ANPD. Fonte: Lei nº 13.709, art. 5º, VIII.

Gestão de Vulnerabilidades: Processo contínuo de identificação, monitoramento, avaliação e eliminação de vulnerabilidades, por meio da realização de testes de vulnerabilidade.

Gestor de Segurança da informação: pessoa responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal.

“Hackeamento”: Consiste na utilização de técnicas para burlar a segurança de um dispositivo com capacidade de processamento de informações, buscando acessá-lo para obter informações, influenciar o seu funcionamento etc.

“Hacking” ético: Atividade executada por qualquer indivíduo que é treinado para dominar tecnologias de “hackeamento” focado em processos de identificação de vulnerabilidades e consequentemente, no desenvolvimento de métodos de proteção. Estes profissionais devem seguir um código de ética para orientar todos os procedimentos.

“Hackeamento” ilegal: Prática de “hackeamento” de forma não ética e considerada crime em vários países, sujeito a punição nos termos de leis nacionais e internacionais. No Brasil as Leis 9.296/19996 e 12.737/2012, podem ser consideradas. Nos EUA, por exemplo, a lei de hacker, assinada por Barak Obama, pode tornar uma pessoa, inconscientemente, um criminoso” (thenextweb.com January 2015).

Hotfix: Pacote cumulativo que inclui um ou mais arquivos que são usados para endereçar um problema num produto de software (isto é, uma parte de software). São feitos para endereçar uma situação específica. Um hotfix, ou mesmo um conjunto de hotfixes, pode ser um pacote usado para corrigir uma série de bugs(falhas), seja em aplicativos ou no próprio sistema. Um exemplo bem tangível são as atualizações de segurança, que objetivam sanar as vulnerabilidades.

Informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

Instrução para o tratamento de dados pessoais: conjunto de regras ou parâmetros que delimitam como os dados pessoais podem ser utilizados ou tratados, desde a coleta até a eliminação;

Malware: Programa de computador destinado a infiltrar-se em um sistema de computador alheio de forma ilícita, com o intuito de causar alguns danos, alterações ou roubo de informações (confidenciais ou não). Ele pode aparecer na forma de código executável, scripts de conteúdo ativo, e outros softwares. "Malware" é um termo geral utilizado para se referir a uma variedade de formas de software hostil ou intruso.

Mapeamento de atividades de dados Pessoais: Processo que permite identificar e documentar os dados pessoais que uma empresa processa e como eles são usados. Importante para garantir que as empresas cumpram suas obrigações legais em relação à proteção de dados pessoais.

Mesa Limpa/Tela Limpa: Mesa limpa e tela limpa se refere a práticas relacionadas de segurança da informação para assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso, ou quando alguém deixa sua área de trabalho, seja por um curto período ou ao final do dia.

Minimização: Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

Multi-Nuvem: estratégia de utilização dos serviços de computação em nuvem por meio de dois ou mais provedor de serviço de nuvem;

Nuvem Comunitária: infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

Nuvem Híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

Nuvem Privada (Ou Interna): infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

Nuvem Pública (ou Externa): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas;

Operador: Art. 5º, VI, da LGPD: Pessoa Jurídica ou Física de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. Art. 39 da LGPD: O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.

Patches: Um tipo de *hotfix* que corrige algo que, por algum motivo, não está funcionando do jeito que deveria dentro de um determinado software. Os patches mais comuns são conhecidos como *bugfix*. Esses são criados e implementados para remediar erros e bugs que se fazem presentes no sistema. Os patches mais comuns têm a ver com vulnerabilidades de segurança. Ou seja, se algum software apresentou uma falha que possa

fazer com que dados importantes sejam vazados ou explorados por criminosos, o patch atua nessa correção.

Plataforma como Serviço (PaaS): tipo de serviço de computação em nuvem, em que o provedor de serviço de nuvem oferece ao cliente a capacidade de operar códigos ou aplicativos personalizados. Um provedor PaaS determina quais sistemas operacionais ou ambientes de execução são oferecidos, não sendo permitido ao cliente modificar os sistemas operacionais (mesmo *patches* de segurança) ou alterar o espaço da rede virtual. A principal vantagem do PaaS é permitir ao cliente reduzir a implantação de hardware em sua própria instalação local e aproveitar um modelo de computação sob demanda (no qual o cliente pagará apenas pelos recursos utilizados);

Princípio da necessidade de conhecer: também conhecido como princípio "*Need-to-know*", aborda o conceito de que um usuário somente deve ter acesso ao que é absolutamente necessário para execução de suas atividades na empresa.

Princípio Menor Privilégio: também conhecido como princípio "*Least Privilege*", aborda o conceito de que um usuário somente deve ter acesso ao que é absolutamente necessário.

Privacidade por Desenho (*Privacy by Design*): É uma abordagem a qual leva em conta a privacidade durante todo o processo de construção de um software ou serviço, considerando os seguintes princípios:

- Pró-ativo não reativo; preventivo não corretivo, de modo a evitar incidentes de violação à privacidade;
- Privacidade como configuração padrão: as configurações padrão de determinado sistema deve ser ajustadas desde o início para preservar a privacidade do usuário;
- Privacidade incorporada ao design, incluindo a arquitetura e modelos de negócio;
- Funcionalidade total - soma positiva, não soma zero;

- Segurança de ponta a ponta: proteção completa incorporada ao ciclo de vida da informação;
- Visibilidade e transparência - mantê-lo aberto;
- Respeito pela privacidade do usuário: mantê-lo centrado nos interesses do usuário.

Privacidade por Padrão (*Privacy by Default*): Diz respeito à adoção da proteção de dados pessoais como padrão em todos os processos e atividades desenvolvidos pela empresa, por meio da definição de medidas de segurança, técnicas e organizacionais que devem ser aplicadas de forma padronizada e constante, em todas as áreas, projetos, produtos. Inclusive verificando se o mínimo necessário em termos de proteção de dados está sendo observado, como finalidade específica e legítima para o tratamento de dados pessoais, ou a minimização dos dados sempre que aplicável.

Provedor de Serviços de Nuvem: ente, público ou privado, que fornece uma plataforma, infraestrutura, aplicativo, serviços de armazenamento ou ambientes de tecnologia da informação baseados em nuvem.

Provisionamento de Serviços: processo de definição de um serviço e do gerenciamento dos dados relacionados, sendo comum em prestação de serviços de computação em nuvem.

Pseudonimização: É o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

PSN: sigla de provedor de serviço de nuvem.

Redes públicas: Redes caracterizadas pelo acesso ao público em geral de forma indistinta disponíveis em locais públicos, como cybercafés, shoppings etc. Também são redes constituídas por entes públicos, como instituições de ensino público, pesquisas governamentais etc. Para o presente Instrumento considera-se o primeiro significado.

Relatório de Atividades de Tratamento de Dados Pessoais: Relatório contendo todas as atividades de tratamento de dados pessoais executadas pela empresa. Também conhecido como ROPA (*Record Of Processing Activities*), este Relatório é um produto do Mapeamento de atividades de dados pessoais.

Relatório de Impacto à Proteção de Dados Pessoais - RIPD: O RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD, às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

SGPI: Sistema de Gestão de segurança da Informação e Privacidade.

SI&P: Segurança da Informação & Privacidade.

SOC 2: desenvolvido pelo *American Institute of CPAs (AICPA)*, define critérios para gerenciamento de dados dos usuários, baseados nos cinco princípios de confiança do serviço - disponibilidade, integridade, confidencialidade, segurança e privacidade - sendo considerado um requisito mínimo a ser atendido pelo provedor de serviço de nuvem. O relatório tipo I informa se o projeto dos sistemas do provedor de serviço de nuvem é adequado para atender os princípios de confiança relevantes. O relatório tipo II detalha a efetividade operacional dos sistemas do provedor de serviço de nuvem.

Software como Serviço (SaaS): tipo de serviço de computação em nuvem em que o provedor de serviço de nuvem oferece ao cliente a capacidade de usar um aplicativo fornecido. São exemplos de SaaS serviços de e-mail on-line e sistemas de edição de documentos on-line. Um usuário de uma solução SaaS só é capaz de usar o aplicativo oferecido e de fazer pequenos ajustes de configuração. O provedor SaaS é responsável pela manutenção da aplicação.

Teste de Vulnerabilidade: Teste ou avaliação de segurança, sem intenção maliciosa ou criminosa, compondo um dos pilares do esforço para tornar a rede corporativa da Companhia mais segura (hacking ético) e identificar vulnerabilidades.

Titular: Qualquer pessoa natural protegida pelo princípio da autodeterminação (Fonte: Lei nº 13.709, art. 2º, II.). Pessoa física cujos dados pessoais são objeto de tratamento pelo Controlador e/ou Operador.

Transferência: Operação de tratamento por meio da qual um agente de tratamento transmite, compartilha ou disponibiliza acesso a dados pessoais a outro agente de tratamento. (Fonte: Resolução CD/ANPD 19 de 23/08/2024). O mesmo conceito pode ser adotado quando os dados não são pessoais.

Transferência Internacional: Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (Fonte: Resolução CD/ANPD 19 de 23/08/2024). O mesmo conceito pode ser adotado quando os dados não são pessoais.

Tratamento de Alto risco: Parâmetro para considerar se uma atividade de tratamento é de alto-risco.

Usuário: Todos os empregados, estagiários, menores aprendizes, terceirizados, que possuem acesso aos ativos de TI e de negócio disponibilizados pela Companhia.

4. FUNDAMENTAÇÃO LEGAL E NORMATIVA

- Política de Segurança e Privacidade e SGPI da Companhia;
- Lei nº 12.737/12: Lei que tipifica crimes cibernéticos ou informáticos:
    a. Invadir dispositivos alheios;
    b. Obter, adulterar ou destruir criminalmente dados;
    c. Instalar vulnerabilidade em dispositivos;
    d. Produzir, oferecer, distribuir, vender ou difundir meios para invasão de dados.
- Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

- Decreto nº 12.572/2025 - Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal.
- Resolução CGPAR/ME Nº 41 de 4/08/2022, que estabelece diretrizes e parâmetros para implementação, desenvolvimento e aperfeiçoamento da Governança de Tecnologia da Informação e Comunicação nas empresas estatais federais.
- Resolução CD/ANPD nº 2/2022: Aprova o Regulamento de aplicação da Lei nº 13.709/2018 (LGPD), para agentes de tratamento de pequeno porte.
- Resolução CD/ANPD Nº 19, de 23/08/2024: Aprova o Regulamento de Transferência Internacional de Dados e o conteúdo das cláusulas-padrão contratuais.
- INSTRUÇÃO NORMATIVA Nº 5, de 30/08/2021: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.
- NC 20/IN01/DSIC/GSIPR: estabelece diretrizes de Segurança da Informação e Comunicações (SIC) para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.
- Legislações internacionais (algumas):
    i. Europa: 2002 Diretiva ePrivacy;
    ii. Europa: 2013 Uma Diretiva sobre ataques contra sistemas de informação. Fonte Web: http://db.eurocrim.org/db/en/vorgang/252/;
    iii. EUA Leis Federais sobre Cybercrime (comportamentos ilícitos
        a. Fraude na Internet;
        b. Pirataria de Software (Roubo de Propriedade Intelectual).
- Referências
    i. ISO/IEC 27001:2013: *Information technology --Security techniques - Information security management systems –Requirements.*
    ii. 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).

iii. ISO/IEC 27701:2019 Versão Corrigida 2020 Information technology -- Security techniques – *Privacy Information Management System (PIMS)* (Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Privacidade da Informação – SGPI).

iv. ISO/IEC 27005:2010: *Information technology --Security techniques - Information security risk management* (Tecnologia da Informação –Técnicas de Segurança –Gerenciamento Riscos Segurança Informação).

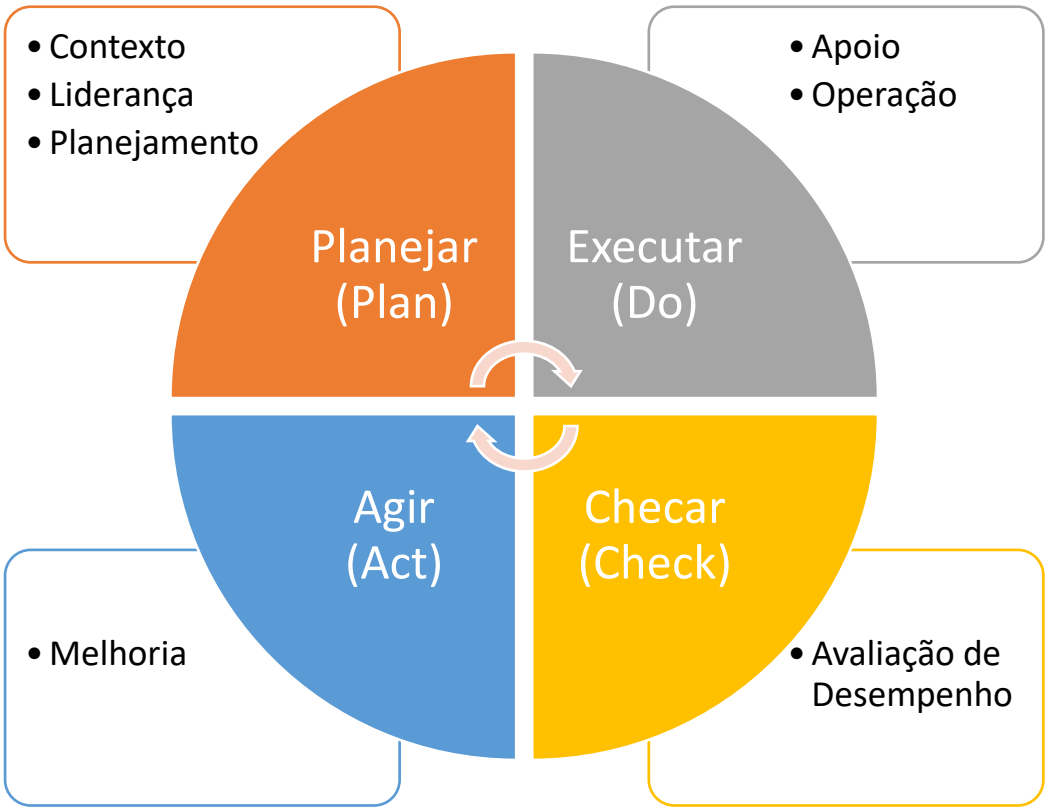
5. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

5.1. INTRODUÇÃO

- Um sistema de gestão representa um conjunto de elementos inter-relacionados que uma empresa estabelece para alcançar objetivos, por meio de políticas e processos. Na disciplina de Segurança da Informação & Privacidade, o respectivo sistema de gestão tem como foco o atingimento de objetivos que visem a proteção das informações e a manutenção da privacidade das pessoas (sob o ponto de vista da proteção dos dados pessoais) e adoção de práticas de conformidade com as legislações pertinentes.
- O presente tópico:
    - descreve o Sistema de Gestão de Segurança da Informação e Privacidade (SGPI), da APS, caracterizado conforme boas práticas (em especial as normas ISO-27001:2022 e ISO-27701:2022 e respectivas estruturas e terminologia).
    - segue (não totalmente) a estrutura apresentada nas normas ISO que são certificáveis, onde os requisitos (ou itens obrigatórios) são documentados e pontuados em processo de certificação (auditoria de certificação ou terceira parte).
    - orienta e/ou facilita processos de auditoria (especialmente as externas) baseados nessas normas.
- Adicionalmente, o SGPI incorpora a visão de Programa de Segurança da Informação, bem como a abordagem de Governança de Segurança da Informação e Privacidade ao

contemplar as funções de governança relativas à orientação, avaliação e monitoramento.

- O SGPI se baseia na metodologia PDCA, tendo cada um de seus itens relacionados com a metodologia, conforme figura abaixo:



5.2. CONTEXTO

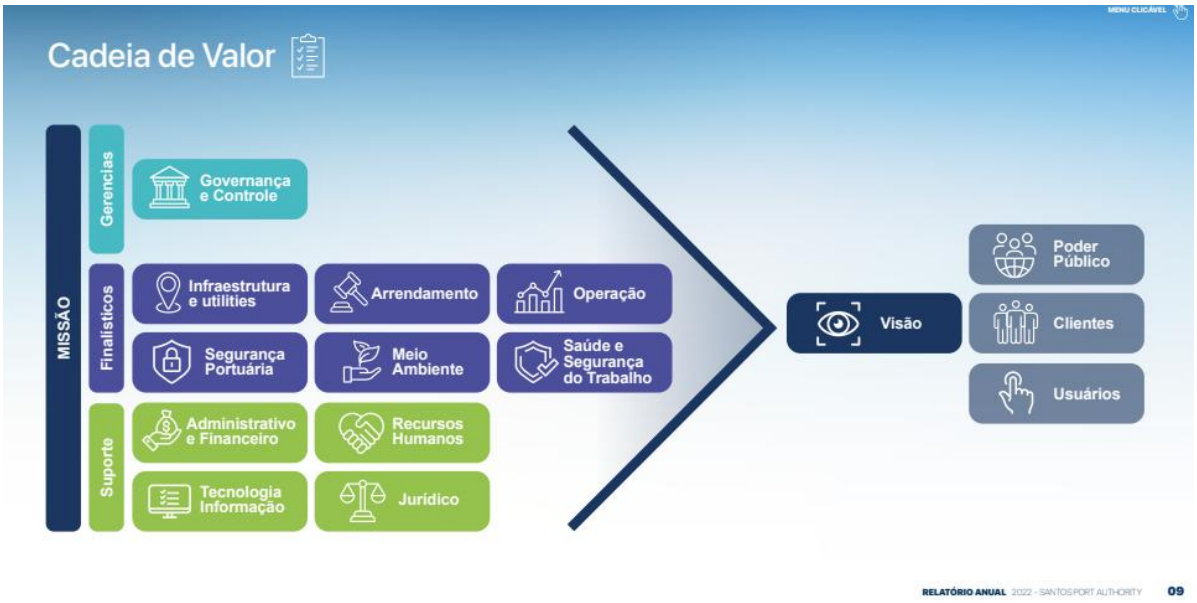
- A APS está instalada na cidade de Santos-SP, e seu objeto social está descrito em seu Estatuto Social.

5.2.1. Partes interessadas

- Os indivíduos ou entidades que têm interesse ou são afetados pelo desempenho e eficácia do SGPI, são:
- Alta administração (DIREXE e CONSAD)
- Órgãos estatutários (COAUD, COPESUR, CONFIS)
- Empregados da APS, Estagiários, Aprendiz

- Empresas que fornecem ou prestam serviço para a APS, através de contratos e outros instrumentos congêneres
- Empresas que prestam serviços na área do Porto Organizado de Santos
- Órgãos reguladores
- Órgão de fiscalização
- Acionistas
- Clientes

5.2.2. Escopo do SGPI



- Compõem o escopo do SGPI, conforme a cadeia de valor da APS:
  - Os processos gerenciais
  - Os processos finalísticos
  - Os processos de suporte

5.3. LIDERANÇA

5.3.1. Declaração de Compromisso da Alta Gestão

- O compromisso da Alta direção está representado pelos objetivos citados na Política de Segurança da Informação e Privacidade.

5.3.2. Declaração de Política de Segurança da Informação e Privacidade

- A Declaração de Política de Segurança da Informação e Privacidade, considera as Disposições Iniciais da Política de Segurança da Informação e Privacidade, que estabelece:
    - Garantir a segurança das informações e a proteção dos dados pessoais dos empregados e seus dependentes, prestadores de serviços e clientes.
    - Garantir a confidencialidade, integridade e disponibilidade das informações, sistemas e dados pessoais, sob sua guarda, além de cumprir com as obrigações legais e regulatórias pertinentes.
    - Promover uma cultura de segurança da informação entre todos os envolvidos, fornecendo treinamento adequado e recursos necessários para mitigar e gerenciar eficazmente os riscos de segurança da informação e de privacidade, buscando a melhoria contínua dos processos e práticas de segurança.

5.4. PLANEJAMENTO

5.4.1. Ações para contemplar Riscos

- As ações para contemplar Riscos consideram o contexto do SGPI da APS e as expectativas das partes interessadas estão voltadas para a mitigação dos riscos aos quais os ativos de Informação estão sujeitos, sob a ótica do gerenciamento de riscos de SI&P.
- O processo de análise e avaliação de risco está definido no manual “SGPI - Análise e Avaliação de Riscos de Segurança da Informação e Privacidade”, inclusive a elaboração da Declaração de Aplicabilidade.

5.4.2. Objetivos do sistema de gestão de SI&P

- Os objetivos do sistema de gestão devem estar alinhados à estratégia corporativa da APS e compor o monitoramento do Plano Diretor de TI.
- Em alinhamento com a estratégia corporativa definida na Política de Segurança da Informação e Privacidade da APS, os objetivos (Vide Anexo – Objetivos do sistema de gestão de SI&P) são:
    - Proteger os dados, dispositivos e sistemas de acesso contra acesso não autorizado e ameaças cibernéticas.

- Garantir a confidencialidade, integridade e disponibilidade das informações.
- Instruir empregados, estagiários e aprendizes sobre práticas de SI&P.
- Garantir a conformidades com Leis e Regulamentos de SI&P.

5.5. APOIO

5.5.1. Recursos

- Recursos financeiros, humanos e técnicos estão alocados para assegurar a eficácia do SGPI, levando em consideração os aspectos organizacionais e o contexto em que a APS está inserida. Os processos de alocação de recursos seguem as normas de compras e aquisições da APS, as quais têm como objetivo atender aos requisitos aplicáveis às empresas estatais.

5.5.2. Competência

- As competências necessárias estão descritas no Manual SGPI no item treinamento e Conscientizações e Anexo I sob a coluna SI&P E GOV.

5.5.3. Conscientização

- Os assuntos ou temas de conscientização e público-alvo estão descritos no Manual SGPI item treinamento e Conscientizações e Anexo I.

5.5.4. Comunicação

- O plano de comunicação do SGPI é uma extensão direta das políticas de segurança da informação e privacidade. Ele abrange a disseminação das informações de segurança da informação, tanto interna quanto externamente, bem como a frequência e os métodos utilizados para compartilhar essas informações. A seguir, são apresentadas as formas de disseminação das informações de segurança, tanto internamente quanto externamente, incluindo a frequência e os métodos pelos quais essas informações são compartilhadas.

  (Atenção: Alguns dos itens seguem os trâmites estabelecidos pelo normativo de Comunicação Social da APS).

Comunicação Interna

Item de comunicação	Iniciador	Destinatário	Frequência	Meio de comunicação
Política, Manuais e outras normas de SI&P	GEPEP	A todos os empregados, estagiários e aprendizes	Ao oficializar	e-mail, publicação na Intranet, verificar visibilidade externa
Indicadores do SGPI	SEGTI	Comite de Segurança da Informação e Privacidade Diretoria Executiva	Conforme tabela Objetivos do SGPI	e-mail
Comunicação de Incidentes	ETIR	Conforme item Gestão de Incidentes do Manual de Gestão de Serviços de TIC	Conforme item Gestão de Incidentes do Manual de Gestão de Serviços de TIC	Conforme item Gestão de Incidentes do Manual de Gestão de Serviços de TIC
Relatórios de Auditoria	SUAUD	Conforme procedimentos da Auditoria Interna	Conforme procedimentos da Auditoria Interna	Conforme procedimentos da Auditoria Interna

Comunicação Externa

Item de comunicação	Iniciador	Destinatário	Frequência	Meio de comunicação
Comunicação de Incidentes	ETIR	Conforme item Gestão de Incidentes do Manual de Gestão de Serviços de TIC	Conforme item Gestão de Incidentes do Manual de Gestão de Serviços de TIC	Conforme item Gestão de Incidentes do Manual de Gestão de Serviços de TIC
Política, Manuais e outras normas de SI&P	GEPEP	A todos os stakeholders	Ao oficializar	Publicação no site do Porto

5.6. OPERAÇÃO

5.6.1. Avaliação e tratamento de Riscos de Segurança da Informação & Privacidade

- O processo de avaliação e tratamento de riscos está descrito no Manual SGPI - Análise e Avaliação de Riscos de Segurança da Informação e Privacidade.

5.7. AVALIAÇÃO DE DESEMPENHO

5.7.1. Monitoramento, medição, análise e avaliação

- Compõe o monitoramento, a apresentação periódica dos indicadores apresentados no Anexo Objetivos do sistema de gestão de SI&P. Outros indicadores de SI&P poderão ser utilizados para monitoramento dos controles de SI&P e analisados conjuntamente.

5.7.2. Auditoria Interna

- Faz parte da avaliação do desempenho do SGPI, as auditorias internas conduzidas na APS sob as condições e planejamento determinado pela SUAUD e dentro de suas atribuições.

5.7.3. Análise crítica pela Direção

- A análise crítica está à cargo do Comite de Segurança da Informação e Privacidade da APS (Regimento interno do CSI Art 6º inciso IX) que se reporta à Diretoria Executiva (Regimento interno do CSI Art. 5º).

5.8. MELHORIA

5.8.1. Não conformidade e ação corretiva

- As não conformidades/recomendações constatadas em processos de auditoria são objeto de ações corretivas. Medidas preventivas e oportunidades de melhoria também são consideradas.

5.8.2. Melhoria Contínua

- Está estabelecido através do presente manual, o compromisso em melhorar continuamente o SGPI, naquilo que couber, considerando as informações apresentadas no item “Monitoramento, medição, análise e avaliação”, bem como outras fontes de avaliação.

6. CONTROLES DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

6.1. CAPACITAÇÃO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE (SI&P)

6.1.1. REFERÊNCIAS CAPACITAÇÃO E CONSCIENTIZAÇÃO DE SI&P

a. Norma Complementar GSI 17/IN01/DSIC/GSIPR Rev. 00 de 09/ABR/13:

I. Atuação e Adequações para Profissionais da Área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

b. Norma ISO-27001 estendida pela ISO-27701

I. item 7.3 Conscientização (ISO-27001) e item 5.5.3 Conscientização (ISO-27701);

II. item A.7.2.2 Conscientização (Anexo A da ISO-27001), educação e treinamento em SI e item 6.4.2.2 (ISO-27701).

c. Controles CIS Versão 8.1 do Center for Internet Security (CIS):

I. Controle 14: Conscientização sobre segurança e treinamento de competências.

6.1.2. DIRETRIZES GERAIS

- A Companhia deve buscar a ampla capacitação e conscientização de matérias relacionadas à SI&P, tanto externamente, quanto internamente.
- Estas ações de capacitação e conscientização devem ser mantidas pelo setor de Segurança da Informação (SEGTI) com apoio das áreas de recursos humanos (GECAR) e comunicação corporativa (SUCOC).
- Capacitações de SI&P devem ser parte integrante do Programa Anual de Capacitação – PRAC da Companhia e ter o tratamento habitual dado pela unidade de gestão responsável pelos treinamentos da Companhia.
- As ações de capacitação e conscientização em SI&P:

  I. Devem permitir a mitigação dos Riscos de SI&P e alinhar a Companhia às boas práticas de mercado, além de atender requisitos regrados pelo Governo Federal.

  II. Podem ser efetivadas por meio de ações de comunicação corporativa, campanhas e treinamentos formais ou informais.

    i. São exemplos de ações de comunicação corporativa: publicações na Intranet, informações na tela inicial dos computadores dos colaboradores, chamadas (publicações, divulgações etc.) no APS+, e-

mails, pôsteres, vídeos e uso de qualquer outro veículo interno de mídia da Companhia.

III. Devem garantir o entendimento das responsabilidades e contribuições de cada parte interessada com a proteção das informações da Companhia, inclusive pessoais.

IV. Devem ter como foco principal a diminuição da probabilidade e impactos da ocorrência de incidentes de SI&P que possam afetar, em qualquer nível, a segurança e privacidade das informações e a continuidade dos processos de negócio da empresa, podendo resultar ou não em sanções contra a Companhia.

V. Devem dar maior atenção e prioridade para empregados e prestadores de serviços da Companhia que exerçam funções específicas e ligadas à SI&P.

VI. Devem, obrigatoriamente, abranger as seguintes partes interessadas:

i. empregados da Companhia, inclusive estagiários, aprendizes, diretores e conselheiros, e seus diferentes perfis de trabalho ligados à SI&P;

ii. prestadores de serviço (principalmente aqueles que tem acesso direto às informações da Companhia), e;

iii. Usuários de Serviços de TIC da Companhia, inclusive os externos.

VII. Os diferentes perfis de partes interessadas que acessam informações da APS devem:

i. Ser capacitados e conscientizados de acordo com as características de sua atuação.

ii. Receber atualizações e reciclagens de conteúdo conforme necessidade.

VIII. Para perfis atuantes diretamente em áreas ligadas à SI&P:

i. As ações podem incluir a participação em fóruns, grupos e listas de discussão.

ii. As ações podem fornecer a preparação de obtenção e a disponibilização de certificação.

IX. Para prestadores de serviços:

i. Os contratos firmados devem estabelecer níveis mínimos de conscientização e capacitação em SI&P por parte da empresa contratada e, em caso de não haver esse mínimo, quando couber, que seja facultada essa formação mínima a ser dada pela Companhia, quanto a: Normas de SI&P da Autoridade Portuária de Santos; Notificação de incidente; Reconhecimento de canal seguro e aplicação autorizada e outras ocorrências.

X. Para usuários de Serviços de TIC da Companhia:

i. Estratégias de conscientização nas interfaces de acesso aos serviços de TIC da Companhia (ex.: banners, rotativos etc.) devem ser adotadas em proporção à importância do serviço.

6.1.3. PERFIS A SEREM CAPACITADOS E CONSCIENTIZADOS

PERFIL	DESCRIÇÃO	QUANDO CAPACITAR
PERFIS GENÉRICOS		
Empregados da Companhia	1. Empregados 2. Aprendizes 3. Estagiários 4. Cargos e Funções de Livre Provimento 5. Diretores 6. Conselheiros	1. Ao ingressar na Companhia. 2. A cada 2 anos.
Prestadores de Serviços	1. Prepostos 2. Empregados, de forma geral, das empresas contratadas pela APS	No início da prestação de serviços ou comprovação no início da prestação de serviços.
Usuários de Serviços de TIC da Companhia	Qualquer pessoa que faça uso de serviços disponibilizados por meio de plataformas tecnológicas.	Ao acessar os serviços de TIC.
PERFIS ESPECÍFICOS LIGADOS À SI&P		
SI&P e Governança	Empregados lotados em setores de SI&P ou com atividades de gestão de SI&P.	1. Ao ingressar na equipe. 2. Periodicamente, obedecendo as prioridades do PRAC.

Segurança Cibernética e Infraestrutura de TIC	Empregados lotados em setores com atividades de segurança cibernética.	1. Ao ingressar na equipe. 2. Periodicamente, obedecendo as prioridades do PRAC.
Central de Serviços e Suporte de TIC	Empregados lotados em setores com atividades de Suporte aos usuários de TIC e Gestão de Serviços de TIC.	1. Ao ingressar na equipe. 2. Periodicamente, obedecendo as prioridades do PRAC.
Desenvolvimento de Software	Empregados lotados em setores com atividades de Desenvolvimento e Manutenção de Sistemas de Informação.	1. Ao ingressar na equipe. 2. Periodicamente, obedecendo as prioridades do PRAC.
Jurídico	Empregados lotados no setor jurídico e com perfil voltado para resposta à ações consequentes de um incidente de SI&P.	1. Ao ingressar na equipe. 2. Periodicamente, obedecendo as prioridades do PRAC.

- Os assuntos que devem ser cobertos nas conscientizações e capacitações de cada um dos perfis estão contemplados no ANEXO I “Conteúdo Programático das Capacitações e Conscientizações de SI&P” deste documento.

6.2. SEGURANÇA NAS OPERAÇÕES

6.2.1. DIRETRIZES GERAIS

- A Superintendência de Tecnologia da Informação (SUPTI) deve elaborar e manter atualizados os Procedimentos Operacionais Padrão (POP) dos procedimentos de operação de TI para:

  I. Instalação e configuração de Sistemas;

  II. Tratamento da informação: processamento automático ou manual;

  III. Cópias de Segurança;

  IV. Tratamento de erros que possam ocorrer durante a execução de uma tarefa;

  V. Contatos para suporte e escalação;

  VI. Manuseio de mídias, formulários especiais, dados confidenciais, descarte seguro e resultados provenientes de falhas de operação;

  VII. Reinício e recuperação de sistemas;

VIII. Gestão de trilhas de auditoria e registros (logs) de sistemas;

IX. Monitoramento.

6.2.2. GESTÃO DE MUDANÇA

- A SUPTI deve definir controles para os seguintes itens:

I. Identificação e registro de mudanças significativas;

II. Planejamento e testes de mudanças;

III. Avaliação de impactos de segurança da informação de tais mudanças;

IV. Procedimentos de aprovação de mudanças propostas;

V. Verificação de que os requisitos de segurança da informação foram atendidos para as mudanças;

VI. Comunicação das mudanças para todas as pessoas relevantes;

VII. Procedimentos de recuperação e responsabilidades para interrupção e recuperação de mudanças em caso de insucesso ou na ocorrência de eventos inesperados;

VIII. Provisão de um processo emergencial de mudança que permita a implementação rápida e controlada de mudanças, necessárias para resolver um incidente.

6.2.3. GESTÃO DE CAPACIDADE

- A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) referentes a:

I. Exclusão de dados obsoletos (espaço em disco);

II. Desativação de aplicações, sistemas, base de dados e ambientes fora de uso;

III. Otimização de processamento em lote;

IV. Otimização da lógica para aplicações ou consultas à base de dados;

V. Gerenciamento da largura de banda para serviços que demandam recursos.

6.2.4. SEPARAÇÃO DOS AMBIENTES DE DESENVOLVIMENTO, TESTE E PRODUÇÃO

- A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) referentes a:

  I. Regras para transferência de código do ambiente de desenvolvimento para o de produção;

  II. Execução de software de desenvolvimento e software de produção em diferentes sistemas ou processadores ou domínios ou partições sempre que possível;

  III. Testes mudanças nas aplicações em ambiente de testes antes de serem aplicadas;

  IV. Não realização de testes em sistemas operacionais;

  V. Utilização de compiladores, editores, ferramentas de desenvolvimento e utilitários de sistemas que não sejam acessíveis aos sistemas operacionais;

  VI. Perfis diferentes para usuários de teste e de produção, com mensagens apropriadas para identificação e redução de erros;

  VII. Impedimento de cópia de dados sensíveis ou pessoais para ambientes de testes sem controles equivalentes de segurança da informação.

6.2.5. PROTEÇÃO CONTRA MALWARE

- É proibido o uso de qualquer aplicação, utilitário ou software não autorizado.
- A SUPTI deve definir e monitorar:

  I. Controles para detectar o uso de software não autorizado em execução;

  II. Controles para detectar acesso a sítios maliciosos, suspeitos, ou de uso contrário às recomendações da Companhia;

  III. Procedimentos Operacionais Padrão (POP) para reduzir vulnerabilidades exploradas por malware através de rotinas de gerenciamento de vulnerabilidades técnicas;

IV. Procedimentos e as responsabilidades no tratamento da proteção contra malware;

V. Planos de Continuidade de Negócios para recuperação em caso de ataques por malware, incluindo cópia de segurança dos dados e sistemas; isolar os ambientes onde impactos negativos possam ocorrer.

- A SUPTI deve executar análises críticas regulares em softwares e dados de sistemas que suportem processos classificados críticos para o negócio, bem como investigar formalmente a presença de qualquer arquivo não aprovado para uso.
- A SUPTI deve instalar e manter software para detecção e remoção de malware em servidores e estações de trabalho incluindo:

I. Varredura em arquivos recebidos;

II. Varredura em e-mail recebidos;

III. Varredura em páginas web.

6.2.6. CÓPIAS DE SEGURANÇA

- A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) de cópias e restauração de dados, considerando:

I. Armazenar as cópias de segurança em locais remotos, a uma distância considerada suficiente para escapar de danos resultantes de um desastre ocorrido no local principal;

II. Proteger física e ambientalmente o local onde as cópias de segurança estão armazenadas, consistentes com as mesmas proteções aplicadas no local principal;

III. Testar regularmente as médias de cópias de segurança, combinado com um teste de restauração;

IV. Criptografar as cópias de segurança que contenham dados classificados como sigilosos.

- Considera-se itens objeto de cópias de segurança:

I. Códigos fontes de sistemas incluindo versionamentos;

II. Bancos de dados (SGBDs e outros arquivos de dados);

III. Scripts;

IV. Caixas postais de e-mails e anexos;

V. Sistemas operacionais e utilitários diversos;

VI. Servidores, principalmente os virtuais;

VII. Configurações diversas de equipamentos;

VIII. Arquivos gerenciados pelo Office 365;

IX. Fotos, vídeos e áudios relacionados às atividades da Companhia;

X. Outros arquivos relacionados às atividades da Companhia.

6.2.7. REGISTROS E MONITORAMENTO

- A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP), bem como manter registros e monitoramento referentes a:

I. Identificação de usuários (ID);

II. Atividades em sistemas;

III. Datas, horários e detalhes de eventos (logon e logout);

IV. Identidade do dispositivo acessado e localização (quando possível);

V. Tentativas de acesso ao sistema (aceitas e rejeitadas);

VI. Tentativas de acesso a outros recursos e dados (aceitas e rejeitadas);

VII. Alterações de configurações do sistema;

VIII. Uso e atribuição de privilégios;

IX. Uso de aplicações e utilitários de sistema;

X. Arquivos acessados e tipo de acesso;

XI. Endereços e protocolos de rede;

XII. Ativação de desativação dos sistemas de proteção (antivírus etc.);

XIII. Registros de transações executadas pelos usuários nas aplicações;

XIV. Proteger de forma adequada com controles de acesso e cópias de segurança todos os registros produzidos.

- A SUPTI deve utilizar uma única fonte de tempo – íntegra – para sincronizar a hora/data de todos os sistemas de processamento de informações, dentro da Companhia ou de seu domínio de segurança.

6.2.8. INSTALAÇÃO DE SOFTWARE EM SISTEMAS OPERACIONAIS

- Somente usuários com direitos e acesso de administradores podem atualizar sistemas operacionais, aplicativos e bibliotecas de programas.
- Sistemas operacionais e de aplicativos só podem ser implementados após testes bem-sucedidos.
- A SUPTI deve manter documentação dos controles sobre a implementação e configuração de sistemas operacionais, bem como implementação de bibliotecas de programas.
- A SUPTI deve manter estratégia de retorno às condições anteriores antes que mudanças sejam implementadas em sistemas operacionais e bibliotecas de programas.
- A SUPTI deve manter registro de auditoria para todas as atualizações das bibliotecas de sistemas e programas.
- A SUPTI deve manter versões anteriores de software aplicativos como medida de contingência.

6.2.9. GESTÃO DE VULNERABILIDADES TÉCNICAS

- A SUPTI deve definir e estabelecer funções e responsabilidades associadas à gestão de vulnerabilidades técnicas, incluindo as atividades de monitoramento, avaliação de riscos, correções, acompanhamento e necessidades de escalação em caso de ocorrência de incidentes.

- A SUPTI deve avaliar os riscos associados e criar Planos de Ação para mitigar estes riscos para cada vulnerabilidade técnica potencial identificada pela área de riscos e controles internos em conjunto com a SUPTI.
- A SUPTI deve avaliar os riscos associados à instalação de correções (*patches* e *hotfix*) disponibilizados.
- A SUPTI deve testar e avaliar as correções disponibilizadas pela TI assegurando sua efetividade. Em caso de não existir a disponibilidade de uma correção, considerar medidas compensatórias:
  I. Desativar os serviços relacionados à vulnerabilidade;
  II. Adaptar ou agregar controles de acesso;
  III. Aumentar a frequência de monitoramento para prevenir ou detectar um ataque real;
  IV. Aumentar a conscientização sobre a vulnerabilidade.
- A SUPTI deve manter registro de auditoria de todos os procedimentos realizados, bem como avaliar e monitorar regularmente o processo de gestão de vulnerabilidades.
- A SUPTI deve priorizar os sistemas críticos de negócio.
- A SUPTI deve alinhar a gestão de vulnerabilidades com a gestão de incidentes, comunicando os dados sobre vulnerabilidades às funções de respostas a incidentes juntamente com Procedimentos Operacionais Padrão caso ocorra um incidente.
- A Gerência de Infraestrutura de Dados (GERID) deve efetuar teste de vulnerabilidade periodicamente a cada 12 (doze) meses, no mínimo, e em caso de:
  I. Mudanças na infraestrutura de TI;
  II. Novos serviços implantados;
  III. Alterações nos serviços existentes;
  IV. Eliminação de vulnerabilidades (verificação de eficácia de medidas de eliminação).

- Ativos de TI da Companhia, que podem ser objeto de varredura para identificação de vulnerabilidades:

  I. Servidores de autenticação;

  II. Servidores de arquivos;

  III. Servidores de aplicação;

  IV. Servidores DNS;

  V. Servidores DHCP;

  VI. Servidores WEB e FTP;

  VII. Servidores de e-mail;

  VIII. Servidores de banco de dados;

  IX. Outros servidores que hospedem outros serviços (exemplo: VPN etc.);

  X. Sistemas Gerenciadores de Banco de Dados (SGBD) e Bancos e/ou instâncias gerenciados por cada um dos SGBD;

  XI. Equipamentos ativos de rede com gerenciamento (*switches*, *gateways*, *firewalls*, roteadores);

  XII. Sistemas *Web-based*;

  XIII. Outros ativos de TI, pertencentes à Companhia e que estejam no ambiente da empresa. Ativos não pertencentes à Companhia, mas que estejam no ambiente da Autoridade Portuária de Santos, devem ser testados em comum acordo com o proprietário e sua participação no planejamento, execução se pertinente, e conclusão.

Observação: Ativos de TI hospedados em nuvem, ou hospedados por terceiros, não devem ser testados por poder caracterizar atividade ilegal (“hackeamento” ilegal). Nesse caso, solicitar evidência quanto a segurança do ambiente.

- É proibida a utilização das ferramentas e técnicas de detecção de vulnerabilidades com o objetivo de invadir e/ou obter qualquer informação de qualquer ativo de TI da Companhia ou de terceiros, de forma ilegal.

- Ferramentas e técnicas devem ser utilizadas para:
  I. Detecção de rede (*sniffing*), cabeada e sem fio;
  II. Varredura para identificação de vulnerabilidades nos ativos de TI;
- Lista (não exaustiva) de vulnerabilidade a serem testadas:
  I. Vulnerabilidades em sistemas *Web-based* (exemplos):
     i. Injeção de SQL;
     ii. Scripts cruzados (cliente e servidor);
     iii. Inclusão de arquivos remotos;
     iv. Sequestro de sessão.
  II. Vulnerabilidades em bancos de dados (exemplos):
     i. Nomes de tabelas de autenticação;
     ii. Acesso a senhas.
  III. Vulnerabilidades em redes sem fio (exemplos):
     i. Chaves de acesso (WEP/WPA);
     ii. Senhas fracas;
  IV. Vulnerabilidades em servidores (exemplos):
     i. Inclusão remota de arquivos;
     ii. *Bind e Black Shells*.
- O planejamento do teste deve considerar:
  I. Indicação do ativo ou ativos a serem testados (candidato a vulnerabilidade).
  II. Indicação do tipo de teste:
     i. Teste caixa preta: Não necessita nenhum conhecimento de estruturas internas ou funcionamento;
     ii. Teste caixa branca: Necessita de conhecimento completo de estruturas internas e funcionamento;
     iii. Teste caixa cinza: Necessita de conhecimento relevante apenas para os testes específicos.
  III. Indicação do ambiente para o teste, inclusive se será feito a partir do ambiente interno e/ou externo, em cópia do ativo de TI para esse fim ou o ativo de TI em SI etc.

IV. Indicação de data e hora para o início do teste, e tempo de duração previsto. Restrições de horários e datas, devem ser considerados.

V. Análise de Risco: Indicação dos riscos, probabilidade e impacto, e medidas de mitigação a serem adotadas preventivamente, e plano de contingência.

VI. Ações de acompanhamento para quando as vulnerabilidades são detectadas.

VII. Indicação de dados armazenados que podem ser acessados durante o teste.

VIII. Formalização de permissão para realização do teste com as indicações citadas e condicionadas ao código de ética EC-council.

IX. Em caso de a realização ser efetuada por terceiros, prever também em contrato:

i. As diferentes leis, diretivas ou regulamentos internacionais, nacionais e locais que podem estar envolvidos.

ii. Proteção contratual contra responsabilidade.

iii. Indenização para cobrir resultados de teste incompletos, como vulnerabilidades não encontradas.

iv. Garantias através de *Non Disclosure Agreement*

v. Cláusula de eliminação de evidências.

- Realização do teste de vulnerabilidade:

I. Iniciar o teste de acordo com o planejado e autorizado, e com as medidas de mitigação de risco executadas;

II. Suspender o teste caso algum risco tenha ocorrido e que não tenha medida de mitigação planejada/executada e/ou plano de contingência;

III. Colher informações necessárias para a realização do teste;

IV. Investigar o ambiente objeto do teste;

V. Explorar as vulnerabilidades possíveis;

VI. Identificar as ferramentas utilizadas, dados utilizados, resultados e evidências da existência/ausência de vulnerabilidade.

- Finalização e conclusão do teste de vulnerabilidade:

I. Eliminar qualquer configuração/ajuste que tenha sido realizado na realização do teste (objetiva-se que nada seja deixado em aberto e que possa se tornar uma vulnerabilidade e ser explorada).

II. Elaborar relatório contendo:

i. O documento do planejamento;

ii. O documento de autorização;

iii. Descrição do teste identificando ferramentas e dados utilizados;

iv. Resultados e evidências das vulnerabilidades encontradas ou não;

v. Para a vulnerabilidades encontradas, avaliação de risco (probabilidade x impacto);

vi. Conclusões;

vii. Recomendações para eliminação das vulnerabilidades encontradas e priorização.

- Eliminação das vulnerabilidades:

I. Adotar ações para eliminação da vulnerabilidade;

II. Evidenciar as ações realizadas;

III. Ressaltar as vulnerabilidades para que as ações de eliminação sejam testadas imediatamente após a eliminação ou em um próximo ciclo de testes.

- Comunicação dos testes de vulnerabilidade: Os relatórios dos testes (tanto os de identificação como os de eliminação) devem ser comunicadas à SUPTI, ao Comitê de Segurança da Informação e à DIREXE.

6.2.10. RESTRIÇÕES QUANTO À INSTALAÇÃO DE SOFTWARE

- A SUPTI deve elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) e Manuais, caso aplicável, estabelecendo os critérios para a instalação de software.

6.2.11. AUDITORIA EM SISTEMAS DE INFORMAÇÃO

- A SUPTI deve planejar e acordar com a Superintendência de Auditoria Interna (SUAUD) as atividades e requisitos de auditoria envolvendo a verificação nos sistemas de forma a minimizar a interrupção nos processos do negócio da Companhia.

- Para minimizar os impactos das atividades de auditoria em sistemas a SUPTI deve:

I. Acordar previamente com a gerência os requisitos de auditoria;

II. Acordar previamente e controlar o escopo dos testes técnicos;

III. Limitar os testes de auditoria para acesso somente de leitura de software e dados;

IV. Acessos diferentes de apenas leitura permitidos somente através de cópias isoladas de arquivos de sistemas e dados. Estas cópias devem ser apagadas após a atividade de auditoria, ou dada proteção adequada se existir a obrigação de guarda de tais arquivos para fins de requisitos de documentação de auditoria;

V. Identificar e acordar previamente requisitos de processamento adicional ou especial;

VI. Realizar fora do horário comercial testes de auditoria que possam afetar a disponibilidade de sistemas de negócio;

VII. Monitorar e registrar todos os acessos de forma a produzir uma trilha de referência.

6.3. SEGURANÇA NAS COMUNICAÇÕES

6.3.1. DIRETRIZES GERAIS

- A SUPTI é responsável pelo gerenciamento e controle das redes para proteger as informações nos sistemas e aplicações da Companhia.
- A SUPTI deve estabelecer e manter controles, bem como elaborar e manter atualizados Procedimentos Operacionais Padrão (POP) para as funções abaixo:

I. Estabelecer funções, responsabilidades e procedimentos para gerenciar os ativos de rede;

II. Se possível, separar a responsabilidade operacional das redes da operação dos recursos computacionais;

III. Estabelecer controles para a proteção da confidencialidade e integridade dos dados que trafegam nas redes internas, públicas e sem fio, bem como sistemas e aplicações a elas conectadas;

IV. Estabelecer controles para manter a disponibilidade dos serviços e dispositivos de processamento de dados conectados;

V. Estabelecer mecanismos de autenticação para todos os sistemas que trafegam nas redes;

VI. Restringir por meios de direito de acesso todas as conexões à rede.

6.3.2. SEGURANÇA PARA OS SERVIÇOS DE REDE

- A SUPTI deve aplicar tecnologias para a segurança dos serviços de redes tais como autenticação, criptografia e controles de conexão de rede.
- A SUPTI é responsável por ativar e manter parâmetros técnicos para conexões seguras com serviços de rede de acordo com regras de segurança para conexão com redes.

6.3.3. SEGREGAÇÃO E REDES

- A SUPTI deve manter segregados grupos de serviços de informação, usuários e sistemas de informação, bem como áreas de desenvolvimento, de testes e de produção.

6.3.4. TRANSFERÊNCIA DE INFORMAÇÕES POR MEIO DE REDES

- A SUPTI quando da transferência de informações por meio de redes:
  I. Protegerá a informação transferida contra interceptação, cópia, modificação, desvio ou destruição;
  II. Detectará e protegerá a informação contra código malicioso que possa ser transferido através da rede;
  III. Protegerá informações classificadas como sigilosas que sejam transmitidas através de anexos de e-mail;
  IV. Especificará o uso aceitável dos recursos de comunicação de dados;
  V. Evitará comprometer a Companhia, através de seus empregados e fornecedores, de difamação, assédio, falsa identidade, retransmissão de “correntes” e notícias falsas, compras não autorizadas etc.;
  VI. Fará uso de criptografia para proteger as informações classificadas como sigilosas transmitidas através das redes;
  VII. Controlará a retransmissão automática de mensagens eletrônicas para endereços externos;

VIII. Orientará os empregados e terceiros, por meio de treinamentos, comunicações, na adoção de precauções apropriadas para não revelar informações classificadas como sigilosas.

- A SUPTI, quando de acordos para transferência de informações, elaborará Procedimentos Operacionais Padrão (POP) ou Manuais, quando aplicável, para:
  I. Responsabilizar os gestores pelo controle e notificação de transmissões, expedições e recepções;
  II. Garantir a rastreabilidade e o não repudio dos eventos;
  III. Elaborar padrões e práticas para embalagem e transmissão de informações;
  IV. Elaborar acordos para procedimentos de custódia;
  V. Proceder à identificação de portadores;
  VI. Determinar funções, papéis e responsabilidades na ocorrência de incidentes de segurança da informação;
  VII. Utilizar um sistema acordado para identificar informações sensíveis e sigilosas garantindo que o significado dos rótulos seja imediatamente entendido, e que esta informação seja ou esteja devidamente protegida;
  VIII. Fazer uso de criptografia para proteção de informações classificadas como sigilosas;
  IX. Manter uma cadeia de custódia para informações em trânsito.

6.3.5. MENSAGENS EM FORMATO ELETRÔNICO

- A SUPTI:
  I. Protegerá as mensagens contra: acesso não autorizado, modificação, negação de serviço, de acordo com o esquema de classificação da Companhia;
  II. Garantirá que o endereço de destino e o meio de transporte de mensagens estejam corretos;
  III. Manterá o serviço disponível e confiável;
  IV. Criará e manterá requisitos de assinatura eletrônica para aspectos legais;

V. Aprovará previamente o uso de serviços públicos externos tais como mensagens instantâneas e de compartilhamento de arquivos;

VI. Manterá níveis mais altos de autenticação para acesso a partir de redes públicas.

6.3.6. ACORDOS DE CONFIDENCIALIDADE E DE NÃO DIVULGAÇÃO

- A SUPTI:

I. Definirá quais informações devem ser protegidas e como serão protegidas;

II. Definirá a duração esperada de um acordo, incluindo situações em que a confidencialidade tenha de ser mantida indefinidamente;

III. Definirá quais ações devem ser executadas ao fim de um acordo;

IV. Definirá as responsabilidades dos signatários do acordo para evitar a divulgação não autorizada da informação;

V. Relacionará a proteção da informação sigilosa com o proprietário da informação, com segredos comerciais e com a propriedade intelectual;

VI. Definirá os direitos do signatário de acordo para fazer uso de uma informação sigilosa;

VII. Auditará e irá monitorar as atividades que envolvem informações sigilosas;

VIII. Criará e manterá um procedimento para notificar e reportar a divulgação não autorizada ou o vazamento de informações sigilosas;

IX. Criará, implementará e manterá regras para retomar ou destruir uma informação ao fim do acordo;

X. Criará e implementará ações e penalidades a serem tomadas no vaso de violação do acordo.

6.4. SEGURANÇA FÍSICA E AMBIENTE

6.4.1. DIRETRIZES GERAIS

- As áreas seguras de TI da Companhia são definidas pela SUPTI e sua definição leva em consideração:

I. Perímetro;

II. Controles de entrada e saída;

III. Salas e outras instalações que não o Data Center.

- O acesso às áreas seguras de TI da Companhia é restrito aos empregados autorizados formalmente pela SUPTI, para desempenho de suas atividades.
- Revisar periodicamente a lista de empregados definidas pela SUPTI, com acesso classificado como sigilosa.
- São considerados Incidentes de Segurança quando ocorre em áreas seguras:

I. Acesso indevido, não autorizado;

II. Abertura, manuseio ou manutenção de ativos de TI sem autorização.

- Incidentes em áreas seguras considerar:

I. Fenômenos naturais;

II. Ações de vandalismo;

III. Qualquer evento de ordem social que gerar risco potencial de indisponibilidade de dados e sistemas ou destruição da área segura.

IV. Sistemas de:

i. Cópias de segurança para os dados processados na área;

ii. Detecção, alertas e extintores de incêndio;

iii. Controles de unidade e temperatura.

- É terminantemente proibido em áreas seguras de TI:

I. Fumar;

II. Beber;

III. Comer;

IV. Documentos impressos, papeis de um modo geral;

V. Produtos inflamáveis;

VI. Qualquer outra atividade que não esteja especificamente vinculada com as atividades de operação e manutenção dos ativos de tecnologia da informação.

- A limpeza e conservação de áreas seguras de TI será realizada:

I. Apenas por profissionais cadastrados e autorizados pela SUPTI;

II. Utilizando-se produtos de limpeza específicos para o ambiente.

- Considerar durante o ciclo de vida dos Ativos e recursos de Tecnologia da Informação:
    - Instalação e Proteção:
        I. Contra falta de energia elétrica e variação de temperatura/umidade;
        II. Local, considerando risco de quedas ou danos de qualquer natureza;
        III. Trancas ou cadeados para impedir acesso indevido ao conteúdo;
        IV. Proteção de cabeamento contra interferências, intervenções ou ataques intencionais que resultem em interrupção de comunicação.
    - Manutenção:
        I. Contrato de Manutenção Preventiva para ativos com risco de indisponibilidade igual ou superior a médio.
    - Reutilização e descarte:
        I. Considerar as diretrizes do tópico Segurança nas Operações e Segurança nas Comunicações deste Manual.
- Segurança de equipamentos e ativos fora das dependências da Companhia.
    I. Supervisionados quando em lugares públicos;
    II. Seguindo as normas do fabricante para a devida proteção do equipamento ou políticas de proteção e classificação para informações;
    III. Avaliação de Riscos para Home Office ou Teletrabalho;
    IV. Registros quando transferidos entre pessoas e/ou locais.
- Considerar:
    I. Mesa limpa;
    II. Tela limpa.

- Será adotada pelos empregados uma política de mesa limpa e tela limpa, que consiste na proteção contra perdas, roubo ou furto de informações sensíveis. As seguintes práticas serão adotadas:
  I. Manter seu local de trabalho, limpo e organizado;
  II. Manter organizados documentos e mídias necessários às atividades do dia a dia, protegidos em pastas, dentro de armários ou gavetas, a fim de evitar que sejam danificadas, destruídas ou mesmo furtadas;
  III. Não expor informações sensíveis, sigilosas, confidenciais ou restritas, tais como: relatórios, propostas comerciais, contratos, dados de clientes, mídias etc.
- Armazenar informações sensíveis, sigilosas, confidenciais ou restritas, em local seguro, trancado com chaves ou cadeado e protegido de acesso não autorizado ou indevido.

6.5. CRIPTOGRAFIA

6.5.1. DIRETRIZES GERAIS

- Informações classificadas de acordo com a tabela de classificação da informação serão armazenadas e transmitidas de forma criptografada, tanto por hardware como por software.
- Informações pessoais classificadas como sensíveis pela LGPD serão armazenadas e transmitidas de forma criptografada por hardware ou por software.
- A Gerência de Carreira e Capacitação (GECAR) em conjunto com a SUPTI deverá promover treinamentos visando capacitar os empregados na atividade de criptografia, bem como instruí-los na atividade de classificação de uma informação.
- Quando da utilização de criptografia de chave pública, caberá exclusivamente à SUPTI o gerenciamento e proteção das chaves privadas.

6.6. PRIVACIDADE POR DESENHO E POR PADRÃO

6.6.1. DIRETRIZES GERAIS

- Deve-se limitar a coleta e o tratamento de dados pessoais ao mínimo que seja relevante, proporcional e necessário para a finalidade a que se destina. Cabe os

princípios da privacidade por desenho e por padrão.

- Onde existir opção de escolha pelo titular, relativo à coleta e/ou tratamento de dados pessoais, que essa opção seja desabilitada por padrão e somente habilitada mediante escolha explicita do titular de Dados Pessoais.
- Deve-se adotar procedimentos para assegurar que os dados pessoais tratados durante o ciclo de vida do dado pessoal, são precisos, completos e atualizados de acordo com as finalidades.
- Deve-se adotar em seus processos de coleta de dados pessoais, a minimização, e quando desnecessário a identificação dos titulares a anonimização ou a pseudonimização.
- Ao final do tratamento, resguardado os requisitos legais pertinentes, deve-se adotar procedimentos para excluir os dados pessoais ou anonimização de forma a não possibilitar a identificação e/ou reidentificação, considerando que os dados pessoais não serão mais necessários.
- Arquivos temporários contendo dados pessoais devem ser descartados.
- Dados pessoais não devem ser retidos por um período além do necessário, de acordo com as finalidades para os quais são tratados.
- Considerar o controle de transmissão de dados pessoais, conforme previsto no tópico de Segurança nas Comunicações deste Manual, observando-se controles pertinentes.

6.7. COMPARTILHAMENTO, TRANSFERÊNCIA E DIVULGAÇÃO DE DADOS E DE DADOS PESSOAIS

- Os dados (inclusive pessoais) a que se refere este item são os gerados pela APS (através de sensoreamento, sistemas internos etc.), os recebidos de terceiros e sob custódia da APS, incorrendo em uma classificação prévia conforme item CLASSIFICAÇÃO DA INFORMAÇÃO, antes do efetivo compartilhamento e/ou divulgação.

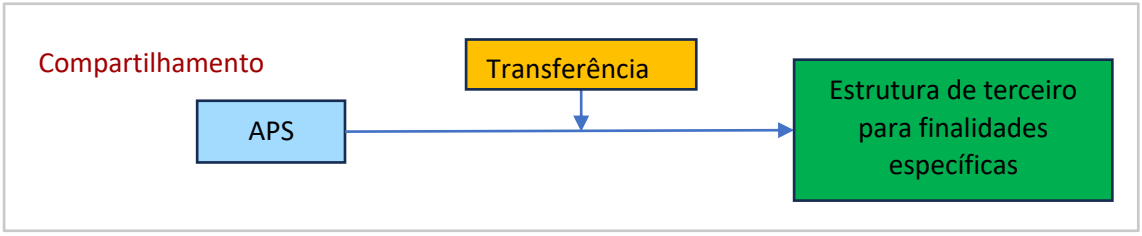


Figura 1- Compartilhamento

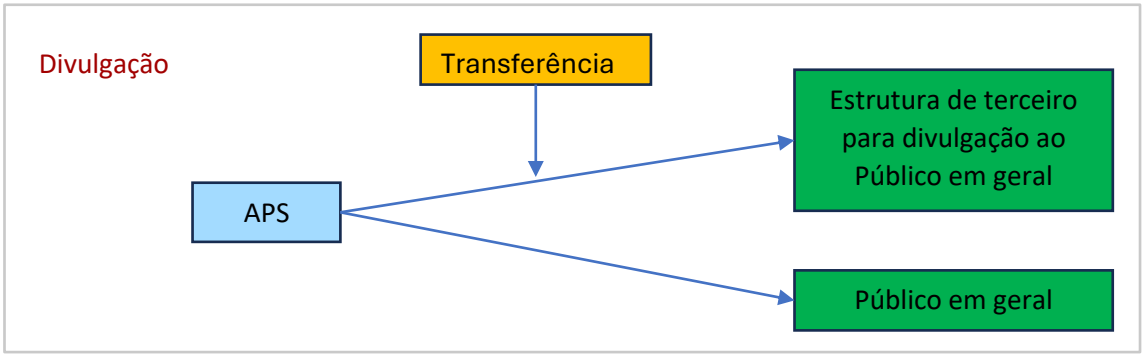


Figura 2 - Divulgação

- O compartilhamento de dados (pessoais ou não) deverá ocorrer conforme requisitos gerais de manipulação de informações (Vide item CLASSIFICAÇÃO DA INFORMAÇÃO, REQUISITOS GERAIS DE MANIPULAÇÃO DAS INFORMAÇÕES), ou seja, para cumprimento de obrigações contratuais ou legais, incluindo investigações legais e/ou auditorias (este último resguardado pelo dever de sigilo ou termos de confidencialidade).
- A divulgação de dados (pessoais ou não) deverá ocorrer conforme diretrizes de classificação da informação (vide item CLASSIFICAÇÃO DA INFORMAÇÃO), cujo tipo de informação for "Público".
- A divulgação de dados (resguardadas as exigências legais inclusive as de proteção de dados pessoais), poderá por interesse da APS, ser via estruturas controladas (ex.: *data-lakes),* acompanhadas por um "termo de Uso", dotadas de controles de segurança e rastreabilidade, destinadas inclusive a compreensão do público demandante, priorização de atendimentos, auditoria e prestação de contas.
- Os dados divulgados (resguardadas as exigências legais inclusive as de proteção de dados pessoais), deverão constar de um catálogo de dados disponíveis, contendo escopo, forma de acesso, classificação, público-alvo e o respectivo termo de uso, ou

na sua ausência, exigências legais, responsabilização pelo uso indevido, divulgação não autorizada ou danos decorrentes.

- A transferência de dados (pessoais ou não) para compartilhamento e/ou divulgação e/ou armazenamento deverá ocorrer conforme diretrizes descritas no item "TRANSFERÊNCIA DE INFORMAÇÕES POR MEIO DE REDES", quando aplicável. Observar no caso de armazenamento, eventuais restrições decorrentes de legislações, políticas e orientações de órgãos reguladores.
- No caso de transferência de dados pessoais para país estrangeiro ou organismo internacional, as diretrizes de transferência internacional de dados pessoais deverão ser observadas (vide item PRÁTICAS DE CONFORMIDADE COM A PROTEÇÃO DE DADOS PESSOAIS, TRANSFERENCIA INTERNACIONAL), antes e enquanto a transferência for necessária para a consecução dos objetivos do tratamento de dados pessoais no qual incorreu a transferência internacional.
- As informações referentes ao compartilhamento, divulgação e transferência internacional de dados pessoais deverão estar devidamente apontadas de forma a fazer parte do Registro das Operações de tratamento de Dados Pessoais (vide item PRÁTICAS DE CONFORMIDADE COM A PROTEÇÃO DE DADOS PESSOAIS, MAPEAMENTO DE ATIVIDADES COM DADOS PESSOAIS).

6.8. FORNECEDORES & SUPRIMENTOS

6.8.1. REFERÊNCIAS PARA FORNECEDORES & SUPRIMENTOS

a. **Resolução CGPAR nº 29 de 05/04/2022:** Estabelece orientações às empresas estatais federais para a contratação de bens e serviços de tecnologia da informação – TI, ou outra norma que vier a substitui-la.

6.8.2. DIRETRIZES GERAIS

- Todas as áreas da Companhia devem endereçar nos contratos a serem celebrados entre a Autoridade Portuária de Santos e seus prestadores de serviço ou fornecedores (e onde aplicável) os seguintes itens:
    - Confidencialidade das informações e continuidade de negócios;
    - Proteção à propriedade intelectual;

- Auditoria e acesso à informação;
- Casos previstos para encerramento do contrato;
- Questões éticas;
- Proteção a Dados Pessoais.

- As diretrizes aqui estabelecidas deverão ser observadas quando da elaboração do Termo de Referência, ou de outro documento que componha o contrato celebrado entre a Companhia e um prestador de serviço e/ou fornecedor.

6.8.3. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE

- Os contratos celebrados entre a Companhia e fornecedores devem seguir as diretrizes de segurança e privacidade elencadas nos itens que seguem.
- Em complemento ao estabelecido no Regulamento Interno de Licitações e Contratos da APS (RILC), os Termos de Referência, quando aplicável, devem prever a apresentação pela contratada de seu Plano de Segurança da Informação relativo aos serviços a serem prestados ou materiais a serem fornecidos, que compreenda itens como controles de acesso, conscientização, gestão de incidentes por parte da contratada (inclusive cobrindo incidentes com dados pessoais da Autoridade Portuária de Santos), logs, guarda de informações e cópias de segurança.
- Quando aplicável, por exemplo em objetos contratuais que envolvam acesso à ativos de informação da Companhia, prever as seguintes obrigações:
  - Promover ações de sensibilização para o pessoal envolvido na execução do contrato, a fim de garantir que estejam informados sobre os instrumentos normativos de segurança da informação vigentes.
  - Disponibilizar apenas empregados com as habilidades de conhecimento e técnicas necessárias em segurança da informação para a realização de tarefas que lhes são confiadas na vigência do Contrato.
- Quando aplicável, por exemplo em objetos contratuais que envolvam ativos de informação da Autoridade Portuária de Santos localizados ou transferidos para locais fora da Companhia, prever as seguintes obrigações, relativas à:
  - Segurança Física:
    - Manter uma lista atualizada das instalações e os edifícios onde as

atividades e resultados são realizados e produzidos.

- Responsabilizar-se por quaisquer potenciais impactos causados pela falta de proteção física.

- Recursos de TI:
  - Proteção contra *Malware*, através de um sistema de proteção contra códigos maliciosos (*Malwares*), considerando que a disseminação deste Malware para os recursos utilizados na vigência do contrato possa afetar a entrega do serviço previsto ou até causar danos aos sistemas de TI da Companhia.
- Rastreabilidade e Monitoração:
  - possuir mecanismos de registro de operações relacionadas com a utilização de recursos de TI para gerar, armazenar, proteger e reproduzir as informações, de modo a registar a origem, a hora e a natureza das operações.
  - realizar análises periódicas do conteúdo dos registros de computador para detectar anomalias e incidentes de segurança.
- Controle de Acesso:
  - possuir mecanismos de identificação e autenticação.
  - possuir sistemas e procedimentos para gerenciar e controlar os direitos de acesso do pessoal agindo em seu nome e acessando recursos utilizados para a realização de atividades contratuais.
  - informar as características de sua política relacionada com a identificação-autenticação de acessos aos recursos, bem como os seus procedimentos de gestão de direitos de acesso, aos seus empregados.
- Gestão de Incidentes de Segurança da Informação e Privacidade:
  - aplicar medidas técnicas e organizacionais para detectar e notificar o mais rapidamente possível os incidentes de segurança que afetam os recursos utilizados para a realização de atividades relacionadas ao contrato, para responder eficazmente, dependendo da natureza dos incidentes de segurança detectados, e atenuar seus impactos, bem como para resolver rapidamente e formalmente todos os incidentes de

segurança.

- alertar a Companhia de qualquer incidente de segurança da informação e privacidade que afete a segurança dos recursos utilizados para a realização de atividades.
- fornecer uma visão geral de todos os incidentes que afetaram a segurança dos recursos.

- Continuidade de Negócios:
  - avaliar os riscos de indisponibilidade dos recursos necessários para a execução de atividades, no âmbito do Contrato, e implementar soluções (técnicas e organizacionais) destinadas a cobrir os cenários de indisponibilidade identificados.
  - fornecer uma descrição dos planos de continuidade de negócios implementados para mitigar os riscos de indisponibilidade dos recursos necessários para a execução de atividades.
- Conformidade:
  - garantir a sua conformidade com todos os requisitos legais e regulamentares aplicáveis a todos os meios utilizados para a realização das atividades previstas, e cobrindo os seguintes campos:
    - Proteção dos dados pessoais e acompanhamento de indivíduos;
    - Propriedade intelectual relacionada a softwares e bancos de dados;
    - Uso de dispositivos de criptografia.

- Quando aplicável, por exemplo em objetos contratuais que envolvam o tratamento de Dados Pessoais, estabelecer (vide Anexo Tratamento de Dados Pessoais):
  - as partes (controlador e operador) envolvidas na contratação de acordo com a LGPD e respectivas responsabilidades. Observar a possibilidade de existência de controladoria conjunta;
  - quais Dados Pessoais (categorias) serão objeto do escopo do contrato;
  - ações de tratamento de Dados Pessoais;
  - medidas de segurança ou requisitos a serem adotadas no tratamento de Dados Pessoais;

- obrigatoriedade de informar ao Controlador sobre qualquer incidente de segurança envolvendo Dados Pessoais;
- ações vinculadas ao encerramento do contrato decorrente do próprio encerramento ou interrupção ou solicitação do controlador;
- condições para participação de terceiros na execução do contrato;
- condições para utilização de recursos de terceiros que implique em transferência internacional de Dados Pessoais. As condições para transferência internacional de Dados estão estabelecidas na Lei nº 13.709/2018 Art. 5 inciso XV, Arts 33 a 36, e em Normativos instituídos pela ANPD;
- proibição de efetuar tratamento de dados pessoais para outras finalidades divergentes da finalidade principal do contrato;
- implementação de meios práticos para permitir que os titulares exerçam seu direito de gerenciamento dos Dados Pessoais.

6.8.4. DIRETRIZES DE COMPUTAÇÃO EM NUVEM

- São considerados soluções baseadas em computação em nuvem as seguintes aplicações:
  - Armazenamento de arquivos
  - Plataformas de Serviços como vídeo chamada, e-mail, streaming, e outras plataformas que disponibilizam soluções na forma de serviços (SaaS, PaaS e IaaS).
- Contratos de computação em nuvem devem prever:
  I. Pelo menos dois data centers localizados no Brasil.
  II. SLAs que contemplem disponibilidade, recuperação de desastres e suporte técnico.
  III. Previsão de auditoria pelo órgão contratante.
  IV. cláusulas contratuais que assegurem segurança da informação, proteção de dados pessoais, auditoria e conformidade com a legislação brasileira;
  V. definição clara das responsabilidades de segurança entre provedor e contratante (modelo de responsabilidade compartilhada);
  VI. garantia de mecanismos de redundância, recuperação de desastres e suporte

técnico;

VII. observância aos normativos do GSI/PR e aos padrões de interoperabilidade

VIII. apresentação obrigatória, pelo provedor de serviços em nuvem, de relatórios de auditoria independentes no padrão SOC 2 (Tipos I e II), como condição de habilitação, manutenção e renovação contratual. no caso de contratação de serviços por intermédio de cloud broker, este deverá apresentar os relatórios SOC 2 referentes a todos os provedores representados.

- Contratos de computação em nuvem devem ser precedidas de avaliação de risco
- Para Dados Classificados (reservados, secretos, ultrassecretos), utilizar somente nuvem privada ou infraestrutura própria.
- Para Dados Pessoais, observar a conformidade LGPD e seus impactos sobre a proteção de dados pessoais
- Para dados Institucionais não classificados pode ser utilizado nuvens públicas, desde que contratada em conformidade com as diretrizes presentes
- Deve-se adotar minimamente os seguintes controles de segurança:
  I. autenticação multifator,
  II. segregação de ambientes,
  III. criptografia em repouso e em trânsito,
  IV. registros de logs e
  V. monitoramento contínuo.
- Periodicamente as soluções em nuvem deverão ser auditadas para verificação de conformidade
- Anualmente deverá ser encaminhado ao Comitê de SI&P, relatório contendo:
  I. inventário de soluções em nuvem utilizadas;
  II. resultados de auditorias e testes;
  III. recomendações de melhorias

6.9. CLASSIFICAÇÃO DA INFORMAÇÃO

6.9.1. REFERÊNCIAS PARA CLASSIFICAÇÃO DA INFORMAÇÃO

a. **Lei 12527/2011 (Lei de Acesso à Informação:** Dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações.

b. **Decreto 7724/2012:** Regulamenta, no âmbito do Poder Executivo federal, os procedimentos para a garantia do acesso à informação e para a classificação de informações sob restrição de acesso, observados grau e prazo de sigilo.

6.9.2. DIRETRIZES GERAIS

- o termo “Classificação da Informação”:

a) Está relacionado aos normativos da APS, relativos à Política de Gestão Documental, Política de Divulgação de Informações, Instrumento Normativo de Processo de Gestão Documental, normativos da CPADs e demais instrumentos que tenham como fundamentação legal a Lei nº 12.527/2011 (Lei de Acesso à Informação). O termo ainda remete ao ato de classificar a informação em grau de sigilo Ultrassecreto, Secreto e Reservado.

b) É referenciado nos principais frameworks de segurança (os quais a APS adota) destinado à proteção das informações conforme seu valor, requisitos legais, sensibilidade etc. a fim de que seja protegida contra modificações e divulgações não autorizadas etc.

c) no presente manual, está descrito como item que visa a proteção das informações na forma prevista nos frameworks de segurança, tendo por aspecto legal a LAI.

- O termo informação, por ser bastante genérico, se aplica a qualquer dado registrado fisicamente ou eletronicamente em qualquer meio físico ou digital.
- É de responsabilidade da APS proteger todos os dados sob sua guarda, incluindo, em especial, aqueles de caráter sigiloso utilizados na execução de suas atividades e tarefas.
- A Superintendência de Tecnologia de Informação (SUPTI) deve implementar, com orientação dos Gestores das informações, os controles tecnológicos necessários e aplicáveis para reduzir fragilidades, e garantir o acesso à informação conforme a classificação da informação e o direito de acesso.

- Devem ser observadas as diretrizes sobre a gestão documental, que estão descritas nos normativos internos da APS.

TABELA CLASSIFICAÇÃO DA INFORMAÇÃO:

Tipo de Informação /Nível de Enquadramento	Restrição de acesso	Descrição	Controle da Confidencialidade/ Publicidade	Controles de segurança/Acesso
Público	Sem restrição	Baixa sensibilidade • Informação com obrigatoriedade de publicização • Informações fornecidas a pedido	N/A	Proteção contra alterações indevidas, preservação da integridade e disponibilidade
Restrito	Sigiloso (Acesso Restrito)	Alta sensibilidade • Dados pessoais e outros dados sujeitos a hipóteses de sigilo previstas em legislações específicas (ex.: médico, fiscal, bancário, de operações e serviços no mercado de capitais, comercial, profissional, industrial, segredo de justiça etc., conforme Art. 6° do Decreto nº 7.724/2012).	Divulgação mediante autorização	Controle de acesso básico como autenticação, permissão baseada em função ou princípio "necessidade de conhecer", Proteção contra alterações indevidas, preservação da integridade e disponibilidade
Classificada	Sigiloso (Classificada)	Altíssima Sensibilidade • Informação com restrição de acesso conforme arts. 23 e 24 da Lei 12527/2011	Restrita Conforme Art. 24 da Lei 12527/2011	Controle de acesso rigoroso, com procedimentos específicos no âmbito da legislação.

- No âmbito interno da APS, as informações devem estar submetidas a medidas de controle de segurança (ou controle de acesso) destinadas para garantir sigilo, inviolabilidade, confidencialidade, integridade, autenticidade e disponibilidade das informações enquadradas conforme Restrição de Acesso.

- Os arquivos digitais que contenham registros de eventos cronológicos relevantes, bem como ações resultantes relativas a um sistema informático (arquivo de log de aplicação) são considerados, por padrão, como “restrito”. Com o apoio da Gerência de Infraestrutura de Dados (GERID) na identificação dos dados armazenados, o seu direito de acesso é passível de mudança caso o gestor do sistema entenda a necessidade.
- Eventualmente as nomenclaturas adotadas neste documento (tabela CLASSIFICAÇÃO DA INFORMAÇÃO) podem ser diferentes das adotadas por sistemas de informação em uso na APS. Nesse caso, deve-se adotar as nomenclaturas dos respectivos sistemas, enquanto estiverem sendo utilizados na APS e documentada na forma de uma tabela de equivalência em relação ao definido no presente documento.

6.9.3. CRITÉRIOS DE ENQUADRAMENTO

- Todas as informações da APS, assim que criadas, devem ter atribuídas o “nível de enquadramento” de acordo com a restrição de acesso definido na tabela acima.
- Cada informação deve ter um nível de enquadramento atribuído por seu respectivo dono (aquele que a criou ou coletou) ou responsável (aquele que mantém a classificação da informação) baseada na tabela acima, de acordo com as necessidades de sigilo ou restrição de acesso de forma a preservar a sua confiabilidade em termos de Confidencialidade, Disponibilidade e Integridade, e requisitos legais.
- O nível de enquadramento de documentos deve ser indicado por marcações no cabeçalho do documento e em todas as páginas (exceto quando público).
- O processo para enquadramento nos níveis “Restrito” e “Classificado” deve estar associado a uma hipótese legal e condicionado a procedimentos específicos definidos na legislação aplicável.

6.9.4. REQUISITOS GERAIS DE MANIPULAÇÃO DAS INFORMAÇÕES

- São requisitos gerais de manipulação de uma informação:
  - **I. Distribuição:**

- Quando não especificado o formato de distribuição em normativos específicos, versões eletrônicas de documentos e/ou informações devem ser disponibilizadas preferencialmente em formato pesquisável e não alterável após a liberação (PDF/A).

II. Armazenamento e Transporte:

- as mídias extraíveis (pen drive, hds externos etc.) que contenham informações com diferentes níveis de enquadramento, devem ser protegidas de acordo com o nível mais sensível;
- antes do transporte de informações em mídias extraíveis, deve haver verificação da existência de outras informações mais sensíveis no dispositivo que não serão transportadas.

III. Rotulagem:

- o rótulo dos meios de informação (mídias de *backup*, e-mail, documento físico etc.) devem identificar o enquadramento da informação mais sensível.

IV. Compartilhamento:

- O compartilhamento de informações com terceiros somente poderá ser realizado para cumprimento de obrigações contatuais ou legais.

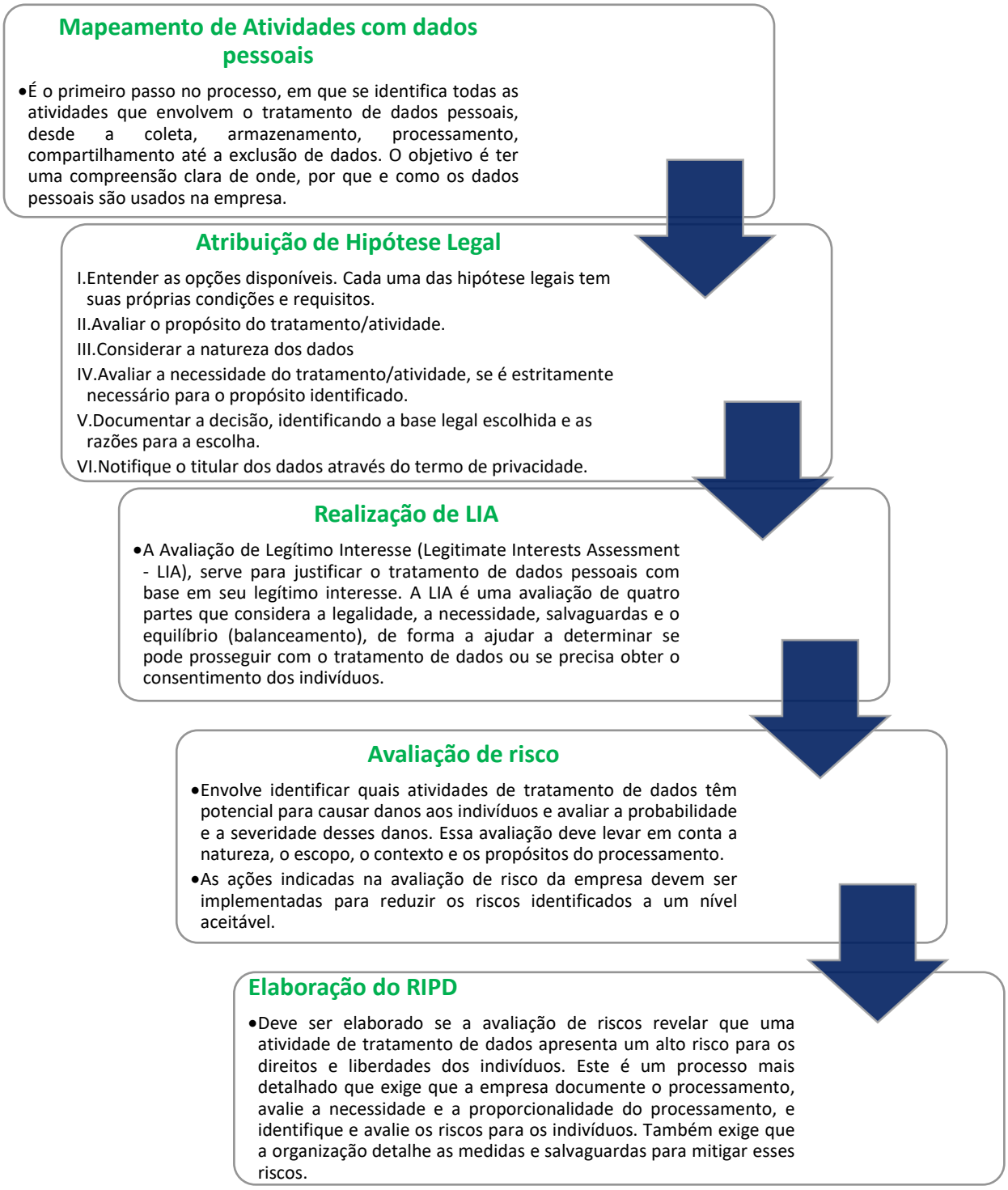
V. Descarte:

- o descarte das informações em formato digital deve considerar a diretriz de tratamento de mídias definidas no Instrumento Normativo de Processo Sistema de Gestão da Privacidade da Informação: Gestão de Ativos, levando em consideração o Instrumento Normativo de Processo de Gestão Documental e a Tabela de Temporalidade da APS.

7. PRÁTICAS DE CONFORMIDADE COM A PROTEÇÃO DE DADOS PESSOAIS

7.1. INTRODUÇÃO

- A conformidade com a proteção de dados pessoais é atingida a partir de um conjunto de práticas, devidamente registradas em artefatos. Sendo elas:



- O resultado dessas práticas pode incidir na criação de projetos e atividades, ou até mesmo na adequação destes.
- Cada prática se subsidia das demais com informações presentes.
- As práticas devem ser executadas regularmente, no mínimo há cada dois anos, para garantir que as mudanças nas operações, nas leis de proteção de dados ou nas

circunstâncias dos indivíduos sejam adequadamente refletidas em suas práticas de tratamento de dados

7.2. MAPEAMENTO DE ATIVIDADES COM DADOS PESSOAIS

- Deve ser executado sempre que uma nova atividade ou projeto que envolva o tratamento de dados pessoais for iniciada. Deve ser mantido atualizado com revisões periódicas, e/ou quando da ocorrência de mudanças na atividade e/ou no projeto, para garantir que as informações estejam atualizadas.
- As unidades de gestão devem informar a SEGTI, sobre novas atividades ou projeto que envolva dados pessoais estiver sendo planejada.
- A coleção de atividades mapeadas compõe um inventário onde considera-se que todas as atividades envolvendo dados pessoais estão identificadas e detalhadas com informações suficientes para elaboração de uma avaliação de risco e do RIPD quando necessário.
- Para cada atividade deve-se identificar suas informações, quais dados pessoais, como eles são tratados e os contratos envolvidos, conforme abaixo:

ATIVIDADES	CONTRATOS
I. Nome, de forma objetiva II.Finalidade/objetivo III.Descrição da atividade IV.Responsável V.Dados de contato (setor, etc)	I. Os contratos (se houver) utilizados na atividade nos quais os dados pessoais são tratados II. Como é ou será a participação de terceiros (contratados e a contratar se for o caso).

DADOS PESSOAIS VINCULADOS À ATIVIDADE

Identificação de Dados Pessoais

I. Quem são os titulares
II. Quais são os dados
III. Quais as categorias
IV. Quem na empresa tem acesso (isto é, compartilhados entre os setores)
V. A hipótese legal conforme Art 7 e 11 da LGPD
   i. Caso Legitimo Interesse, fazer a Análise de Legitimo Interesse para saber se é possível utilizar essa base.

Origem dos dados

I. Como esses dados são obtidos, quem as obtém e com que periodicidade
II. Quem as obtém os dados
III. Qual é a periodicidade de obtenção

Destinação dos Dados

I. Onde esses dados são armazenados
II. Por quanto tempo os dados são armazenados
III. Como e quando as informações são eliminadas (descartadas)
IV. Quais são os sistemas (se houver) que são utilizados na atividade
V. Com quem, como e quando as informações são compartilhadas (para fora da Companhia)
VI. Quais os países para os quais as informações são transferidas (se houver)

Segurança

I. Quais são as medidas de segurança aplicadas na atividade

- Para cada contrato deve-se avaliar:

A existência de clausulas de privacidade	Indicação de controlador, operador ou controladoria conjunta	A existência das instruções de tratamento de dados pessoais
A previsibilidade da destinação dos dados pessoais após o encerramento do contrato	O poder de decisão sobre o tratamento de dados pessoais da atividade em análise a existência de interesses mútuos sobre os dados pessoais da atividade em análise.	A existência de interesses mútuos sobre os dados pessoais da atividade em análise.

7.3. AVALIAÇÃO DE LEGÍTIMO INTERESSE

- Caso a hipótese legal considerada para a atividade seja a de Legítimo Interesse, a Superintendência Jurídica (SUJUD) deve fazer a avaliação para confirmar a aplicabilidade dessa hipótese segundo os critérios:
- Quanto à Legitimidade (referência: art. 10, caput, LGPD):
    I. O tratamento de dados deve ter uma finalidade legítima, ou seja, não deve contrariar nenhum dispositivo legal.

II. A finalidade do tratamento de dados deve ser específica, explícita e informada ao titular (referência: art. 6, I, LGPD).

III. A situação em que os dados serão tratados deve estar claramente definida e articulada.

- Quanto à Necessidade (referência: art. 10, § 1º, LGPD):
  I. O tratamento de dados deve ser limitado ao mínimo necessário para a realização de suas finalidades.
  II. A quantidade de dados pessoais coletados deve ser a mínima necessária para atingir a finalidade.
- Quanto ao Balanceamento (referência: art. 10, I e II, LGPD):
  I. O tratamento de dados deve apoiar e promover atividades legítimas do controlador.
  II. O tratamento de dados deve proteger e respeitar os direitos e as expectativas legítimas do titular.
  III. O tratamento de dados pessoais não deve surpreender o titular, ou seja, deve estar alinhado com as expectativas que o titular tem com base na relação prévia com o agente de tratamento.
- Quanto às Salvaguardas (referência: art. 10, § 2º, LGPD):
  I. O controlador deve ter medidas em vigor para garantir a transparência do tratamento de dados baseado no legítimo interesse.
  II. O titular deve ter a oportunidade de exercer o direito de oposição ao tratamento de dados, se assim o desejar.
- Caso qualquer critério não seja atendido a hipótese legitimo interesse não pode ser considerada, devendo-se rever a indicação.

7.4. AVALIAÇÃO DE IMPACTO À PRIVACIDADE DO PROCESSO DE TRATAMENTO DE DADOS PESSOAIS

- Deve ser executado pela SEGTI, sempre que uma nova atividade ou projeto que envolva o tratamento de dados pessoais for iniciada. Deve ser mantido atualizado com revisões periódicas, e/ou quando da ocorrência de mudanças na atividade e/ou no projeto.

- Para cada atividade ou grupo de atividades que faça parte de um processo:
    I. Identificar e analisar os impactos à privacidade (ou riscos potenciais para a privacidade) dos titulares dos dados pessoais envolvidos.
    II. Avaliar a probabilidade e o impacto dos riscos identificados.
    III. Indicar medidas de mitigação para reduzir ou eliminar os riscos identificados.
    IV. Definir ações a serem implementadas para garantir a conformidade com os requisitos de privacidade.

7.5. RELATÓRIO DE IMPACTO À PROTEÇAO DE DA PESSOAIS (RIPD)

- O RIPD é o documento formal representativo do mapeamento e da avaliação de risco.
- A SEGTI deve avaliar a necessidade/obrigatoriedade de elaboração do RIPD, segundo os critérios:
    I. Caso seja um processo ou tratamento de alto risco
        i. Conforme Art. 4, res. CD/ANPD nº2/2022 tratamento de Alto Risco leva em consideração:
            a. critério geral (“larga escala” ou “afetar significativamente interesses e direitos fundamentais dos titulares”).
            b. critério específico (“uso de tecnologias emergentes ou inovadoras”, “vigilância ou controle de zonas acessíveis ao público”, “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais” ou “utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos”).
            c. A existência de pelo menos um critério geral e um critério específico é considerado de alto risco.

II. Tratamento com hipótese legal como sendo Legitimo Interesse;

III. Solicitação da Autoridade Nacional de Proteção de Dados (ANPD).

- Caso a avaliação indique a necessidade de elaboração do relatório, a SEGTI deve elaborar o relatório a partir do mapeamento e da avaliação de risco contendo:

I. Identificação dos agentes de tratamento e do encarregado;

II. Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos;

III. Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros);

IV. Projeto/Processo que justifica a elaboração do RIPD;

V. Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD;

VI. Tratamento de dados:
   a. Descrição do tratamento (desde a coleta até a eliminação);
   b. Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa);
   c. Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados de forma completa);
   d. Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços);
   e. Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver;
   f. Volume de dados pessoais tratados e número de titulares envolvidos no tratamento;
   g. Fonte de coleta;
   h. Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado);
   i. Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver);
   j. Política de armazenamento (descrever os prazos de retenção e métodos de descarte);

VII. Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento;

VIII. Análise de princípios da LGPD;

IX. Riscos identificados ao titular;

X. Resultado apurado com base na metodologia utilizada pelo agente de tratamento:
   a. Descrição do Risco e do Impacto para os titulares
   b. Probabilidade
   c. Impacto
   d. Risco Total

XI. Medidas, salvaguardas e mecanismos de mitigação de risco:
   a. Risco
   b. Tratamento de Risco (descrição das medidas adotadas para redução do risco)
   c. Risco após o tratamento
   d. Risco Residual

XII. Comentários e aprovações.

7.6. TRATAMENTO DE DADOS PESSOAIS ATRAVÉS DE COOKIES

- A utilização de cookies nos sites internet/intranet, durante o tempo que o usuário navega em um site, é uma prática bem difundida e útil. Ela possibilita e facilita a iteração do usuário com o site (e outros sites).
- Existem várias classificações dos cookies conforme o objetivo aplicação e destinação a saber (fonte: guia Cookies e Proteção de Dados, da ANPD):

I. Cookies próprios ou primários: são os cookies definidos diretamente pelo site ou aplicação que o usuário está visitando. Esses tipos de cookies podem incluir informações como credenciais de login, itens do carrinho de compras ou idioma preferido.

II. Cookies de terceiros: são cookies criados por um domínio diferente daquele que o titular está visitando. Decorrem de funcionalidades de outros domínios que são incorporadas a uma página eletrônica, a exemplo da exibição de anúncios.

III. Cookies necessários: são aqueles utilizados para que o site ou aplicação realize funções básicas e opere corretamente.

IV. Cookies não necessários: são cookies que não se enquadram na definição de cookies necessários e cuja desabilitação não impede o funcionamento do site ou aplicação ou a utilização dos serviços pelo usuário.

V. Cookies analíticos ou de desempenho: possibilitam coletar dados e informações sobre como os usuários utilizam o site, quais páginas

visitam com mais frequência naquele site, a ocorrência de erros ou informações sobre o próprio desempenho do site ou da aplicação.

VI. Cookies de funcionalidade: são usados para fornecer os serviços básicos solicitados pelo usuário e possibilitam lembrar preferências do site ou aplicação, como nome de usuário, região ou idioma. Os cookies de funcionalidade podem incluir cookies próprios, de terceiros, persistentes ou de sessão.

VII. Cookies de publicidade: são utilizados para coletar informações do usuário com a finalidade de exibir anúncios. Mais especificamente, a partir da coleta de informações relativas aos hábitos de navegação do usuário, os cookies de publicidade permitem sua identificação, a construção de perfis e a exibição de anúncios personalizados de acordo com os seus interesses.

VIII. Cookies de sessão ou temporários: são projetados para coletar e armazenar informações enquanto os usuários acessam um site. Costumam ser descartados após o encerramento da sessão, isto é, após o usuário fechar o navegador. São utilizados regularmente para armazenar informações que só são relevantes para a prestação de um serviço solicitado pelos usuários ou com uma finalidade específica temporária, como ocorre, em geral, com uma lista de produtos no carrinho de um site de compras.

IX. Cookies persistentes: os dados coletados por meio desses cookies ficam armazenados e podem ser acessados e processados por um período definido pelo proprietário do site, que pode variar de alguns minutos a vários anos.

- Dependendo das informações armazenadas nos cookies e o que motiva o armazenamento pode ser considerado tratamento de dados pessoais e, portanto, sujeito às práticas de proteção de dados.
- O Painel de gerenciamento de cookies permite que o titular dê o consentimento para o tratamento de dados pessoais e ainda demonstra os princípios de livre acesso e de transparência, para essa atividade de tratamento.

- Recomenda-se que os sites construídos:
    I. Tenham um “painel de gerenciamento de cookies” onde:
        a) se elenquem os tipos de cookies utilizados, quais dados são armazenados, suas finalidades, e se são próprios ou de terceiros
        b) Excetuando o Cookie Necessário, permita ao usuário escolher quais tipos de cookies ele autoriza ou não que sejam armazenados ou controlados pelo site
        c) As opções de autorizar/não autorizar devem estar desmarcadas (não autorizar)
    II. Tenham os dados de seus cookies persistentes armazenados por um tempo mínimo necessário;
    III. Tenham seus cookies necessários, avaliados quanto aos princípios da LGPD de finalidade, necessidade, adequação, livre acesso e da transparência.
    IV. Elenquem no Termo de Privacidade do Site, em tópico específico, os cookies utilizados, quais dados são armazenados, suas finalidades e se são próprios ou de terceiros, bem como a possibilidade de gerenciamento (ou consentimento).
- Os sites construídos pela APS ou sob sua gestão, devem observar as recomendações acima sobre o Painel de gerenciamento de cookies e termo de privacidade.
- Apesar do usuário poder se opor a utilização de cookies desativando a opção correspondente no navegador internet de seu computador ou dispositivo móvel, efeitos colaterais podem ocorrer como o não funcionamento correto de algumas funcionalidades, não registro de preferencias, prejuízo à experiencia de navegação etc.

7.7. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

- A transferência internacional de dados pessoais faz parte de uma atividade de tratamento de dados pessoais a qual deve apresentar as características de conformidade (transparência, adequação, direitos do titular etc.) com a LGPD e por consequência é refletida na transferência internacional.

- A possibilidade da utilização da transferência internacional deve ser avaliada (de acordo com a norma de Transferência Internacional aprovada pela ANPD, por resolução vigente na ocasião) previamente e enquanto for necessária para a consecução dos objetivos do tratamento de dados pessoais no qual incorreu a transferência internacional.
- A Transferência Internacional de Dados Pessoais somente poderá ser utilizada nos seguintes casos:
    I. para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei nº 13.709, de 14 de agosto de 2018, mediante reconhecimento da adequação pela ANPD; ou
    II. quando controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei nº 13.709, de 14 de agosto de 2018, na forma de:
        - cláusulas contratuais específicas para determinada transferência (conforme aprovação ou reconhecimento pela ANPD de acordo com procedimento próprio);
        - cláusulas-padrão contratuais (conforme resolução aprovada pela ANPD de acordo com procedimento próprio);
        - normas corporativas globais destinadas a organizações do mesmo grupo (conforme aprovação da ANPD de acordo com procedimento próprio);
        - nas demais hipóteses previstas em Lei.
- Deverá ser adotada nas formalizações contratuais que incorrerem em Transferência Internacional, as cláusulas definidas e aprovadas pela ANPD, por resolução vigente na ocasião.
- A ANPD poderá reconhecer através de uma “Decisão de Adequação” a equivalência do nível de proteção de dados pessoais de país estrangeiro ou de organismo internacional com a legislação nacional de proteção de dados pessoais.

8. PAPÉIS E RESPONSABILIDADES

8.1. PAPÉIS E RESPONSABILIDADES ESPECÍFICOS DAS ATIVIDADES DESSE MANUAL

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE	
Unidade de Gestão	**Responsável por/pela(as):**
SEGTI	Responsável por conduzir ações de melhoria do SGPI

CAPACITAÇÃO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE (SI&P)	
Unidade de Gestão	**Responsável por/pela(as):**
GECAR	Operacionalização de treinamentos, externos e internos, e inclusão dos treinamentos de SI&P no PRAC.
SUCOC	Ações de comunicação social no âmbito da Companhia, direcionado ao público interno.
SUPTI	Área da Companhia onde se encontram as equipes de Segurança da Informação & Privacidade e Cyber segurança. Responsável pelo controle e requisição da realização dos treinamentos/conscientizações.
Empregados	Participar dos treinamentos de SI definidos pela SUPTI.

SEGURANÇA NAS OPERAÇÕES	
Unidade de Gestão	**Responsável por/pela(s):**
SUPTI	Aplicação das políticas e práticas de Segurança da Informação. Responsável pelos controles tecnológicos que apoiam a proteção da informação de todas as Unidades de Gestão da Companhia, nos aspectos de: • identificação; • apresentação; • sustentação; • escolha; • implantação; e, • manutenção.
GERID	Realizar os testes de vulnerabilidade.

SEGURANÇA NAS COMUNICAÇÕES

Unidade de Gestão	Responsável por/pela:
SUPTI	Aplicação das políticas e práticas de Segurança da Informação. Responsável pelos controles tecnológicos que apoiam a proteção da informação de todas as Unidades de Gestão da Companhia, nos aspectos de: • identificação; • apresentação; • sustentação; • escolha; • implantação; e, • manutenção.

SEGURANÇA FÍSICA E AMBIENTE	
Unidade de Gestão	**Responsável por/pela:**
SUPTI	Identificação, escolha, implantação e manutenção dos controles tecnológicos que apoiam a proteção das áreas, ambientes e ativos de informação em todos os departamentos dentro da Companhia.
GERID	Controlar acesso às áreas seguras.

CRIPTOGRAFIA	
Unidade de Gestão	**Responsável por / pelo:**
SUPTI	Gerenciamento das chaves públicas de criptografia.
SECURITY OFFICER (RESPONSÁVEL PELA SEGURANÇA DA INFORMAÇÃO)	Empregado oficialmente nomeado e responsável pela manutenção do Sistema de Gestão da Privacidade da Informação (SGPI).
GECAR	Operacionalização de treinamentos na utilização de criptografia.

PRIVACIDADE POR DESENHO E POR PADRÃO, ANONIMIZAÇÃO E PSEUDOMINIZAÇÃO	
Unidade de Gestão	**Responsável por / pelo:**
TODAS AS ÁREAS	Observar as diretrizes nas atividades em que ocorrem Dados Pessoais e nas atividades e/ou projetos em estudo que envolvam dados pessoais. Observar item Práticas de Conformidade com a Proteção de Dados Pessoais.

FORNECEDORES E SUPRIMENTOS

Unidade de Gestão	Responsável por/pelo:
GEJAD	Alinhar as cláusulas contratuais padrão com as diretrizes deste manual e do RILC.
GELIC	Aplicar as cláusulas contratuais padrão nos contratos e editais de licitação.
TODAS AS ÁREAS	Observar as diretrizes nas atividades em que ocorrem Dados Pessoais e nas aquisições (bens ou serviços) que envolvam dados pessoais. Observar item Práticas de Conformidade com a Proteção de Dados Pessoais.
ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS	Orientar as áreas de negócio a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

PRÁTICAS DE CONFORMIDADE COM A PROTEÇÃO DE DADOS PESSOAIS	
Unidade de Gestão	**Responsável por/pelo:**
SEGTI	Realizar e Manter o mapeamento e avaliação de riscos atualizados, verificar a necessidade de elaboração do RIPD, elaborar e manter atualizado o RIPD. Auxiliar a SUJUD em relação a atribuição de Hipóteses Legais e a Avaliação de Legítimo Interesse. Auxiliar as áreas de negócio.
SUJUD	Analisar os mapeamentos e atribuir Hipótese Legal e se necessário fazer a Avaliação de Legitimo Interesse. Auxiliar na elaboração do RIPD.
DIREXE	Analisar e Aprovar o RIPD.
UNIDADES DE GESTÃO COM ATIVIDADES COM DADOS PESSOAIS	Colaborar na elaboração do mapeamento de dados pessoais, informar a SEGTI sobre alterações nas atividades mapeadas e implementar as ações de mitigação de riscos à privacidade, apontadas na avaliação de riscos. Auxiliar na realização da avaliação de risco e na elaboração do RIPD.
ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS	Opinar sobre o RIPD. Orientar os empregados e os contratados da Companhia a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

8.2. PAPÉIS E RESPONSABILIDADES GENÉRICOS

Neste item estão descritas as atividades esperadas por cada um dos atores abaixo, mencionadas em legislações aplicáveis a cada um. Eventualmente parte das atividades estão também mencionadas nos quadros do item anterior e não caracterizam duplicidade, mas consolidação, pois as descrições abaixo podem ser mais abrangentes em relação aos quadros acima.

8.2.1. Gestor de Segurança da Informação

O Gestor de Segurança da Informação é a pessoa responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal. Tem as seguintes funções:

- participar da elaboração de normas e procedimentos internos de tratamento da informação;
- receber relatório mensal sobre a utilização de mídias sociais;
- receber relatório sobre incidentes de segurança ocorridos nos perfis institucionais;
- propor ações para melhoria contínua da gestão do uso seguro de mídias sociais;
- fomentar o fortalecimento da cultura da segurança da informação no seu respectivo órgão ou entidade, no que diz respeito ao uso seguro de mídias sociais;
- designar o agente responsável pelo uso seguro de mídias sociais;
- instituir e coordenar a equipe responsável pela elaboração e pelas revisões do ato normativo sobre o uso seguro de mídias sociais;
- apresentar o relatório sobre a utilização de mídias sociais à alta administração e ao Comitê de Segurança da Informação ou à estrutura equivalente;
- encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de mídias sociais;
- responsável por planejar, implementar e melhorar continuamente os controles de segurança da informação em ativos de informação;
- receber pedidos de autorização de acesso aos recursos corporativos através de dispositivo móvel particular;

- coordenar o uso dos Dispositivos Móveis, bem como indicar Agente Responsável pela gerência das atividades de uso de dispositivo móvel particular;
- prover os meios necessários para a infraestrutura necessária, capacitação e o aperfeiçoamento técnico dos membros da ETIR;
- instituir e coordenar a equipe para elaboração e revisões de ato normativo sobre uso seguro de computação em nuvem;
- supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;
- assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao órgão ou à entidade, de forma a assegurar que os controles e os níveis de serviço de computação em nuvem acordados sejam cumpridos;
- supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;
- comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;
- encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem;
- coordenar o processo de mapeamento de ativos de informação, bem como designar um agente responsável pela gestão dos ativos de informação;
- receber o relatório de identificação, análise e avaliação dos riscos de segurança da informação (atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo), para aprovação;
- coordenar a gestão de riscos de segurança da informação;
- designar o agente responsável pela gestão de riscos de segurança da informação;
- aprovar o plano de gestão de riscos de segurança da informação;
- aprovar o relatório de identificação, análise e avaliação dos riscos de segurança da informação e encaminhá-lo à alta administração;
- aprovar o relatório de tratamento de riscos de segurança da informação;

- propor medidas preventivas à alta administração;
- coordenar o processo de gestão de continuidade de negócios em segurança da informação, bem como designar um agente responsável pela referida gestão;
- coordenar a gestão de mudanças no aspecto de SI gestão;
- designar o agente responsável pela gestão de mudança;
- analisar e encaminhar o documento de avaliação e aprovação de mudança para apreciação da alta administração do órgão, à qual cabe a decisão de aprovar ou indeferir a mudança;
- proporcionar a interação constante entre as equipes de gestão de mudanças em aspectos de segurança da informação, de gestão de riscos de segurança da informação e de gestão de continuidade de negócios em segurança da informação;
- analisar o documento de avaliação e aprovação de mudança elaborado juntamente com o grupo técnico de mudança;
- receber informação sobre o andamento e a conclusão do processo;
- fornece, ao(s) agente(s) responsável(is) pela avaliação de conformidade, todas as informações necessárias ao processo de gestão de conformidade nos aspectos de segurança da informação;
- emitir parecer técnico sobre o relatório de avaliação de conformidade e apresentá-los ao Comitê de Segurança da Informação;
- adotar as medidas necessárias para atender às recomendações do relatório de avaliação de conformidade aprovado pela alta administração;
- coordenar a elaboração da Política de Segurança da Informação com a participação do Comitê de Segurança da Informação;
- promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos;
- coordenar a elaboração da Política de Segurança da Informação e das normas internas de segurança da informação do órgão, observadas as normas afins

exaradas pelo Gabinete de Segurança Institucional da Presidência da República e as melhores práticas sobre o assunto;

- assessorar a alta administração na implementação da Política de Segurança da Informação;
- estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
- promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;
- incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação;
- propor recursos necessários às ações de segurança da informação;
- acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;
- verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;
- acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;
- manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação;
- compor o Comitê de Segurança da Informação;
- implementar os procedimentos relativos ao uso de recursos criptográficos, em conformidade com as orientações contidas na norma e deve possuir credencial de segurança;
- receber da ETIR em função do tipo e do impacto, os dados relativos ao incidente cibernético.

São disciplinas associadas:

- CONTINUIDADE DE NEGÓCIOS - capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, a fim de manter suas operações em um nível aceitável, previamente definido;
- ANÁLISE E AVALIAÇÃO DE RISCOS: no contexto do presente manual se refere ao processo sistemático que envolve etapas estruturadas para identificar, analisar, medir e priorizar os riscos (de segurança da informação e privacidade) que podem afetar a confidencialidade, integridade e disponibilidade das informações de uma organização. Apesar desse processo ser comum a várias disciplinas, o presente manual se refere exclusivamente aos riscos de segurança da informação e privacidade;
- GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SEGURANÇA DA INFORMAÇÃO - processo estruturado que visa aumentar a probabilidade de sucesso em mudanças, com mínimos impactos, e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;
- GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO - processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
- GESTÃO DE SEGURANÇA DA INFORMAÇÃO - processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;
- GESTÃO DE INCIDENTES CIBERNÉTICOS - processo que realiza ações sobre qualquer evento adverso relacionado à segurança cibernética dos sistemas ou da infraestrutura de computação;
- GESTÃO DE ATIVOS - processo estratégico e sistemático de monitorar, controlar, otimizar e proteger todos os recursos tecnológicos de uma organização ao longo de seu ciclo de vida, desde a aquisição até o descarte. Visa conhecer os recursos tecnológicos de forma a protegê-los adequadamente;

- AVALIAÇÃO DE CONFORMIDADE DE SEGURANÇA DA INFORMAÇÃO - exame sistemático do grau de atendimento dos requisitos relativos à segurança da informação com legislações específicas.

8.2.2. Encarregado pelo Tratamento de Dados Pessoais

O encarregado é uma pessoa indicada pelo controlador e operador (pessoa natural, integrante do quadro organizacional do agente de tratamento ou externo a esse; ou uma pessoa jurídica) para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), sendo capaz de comunicar-se com os titulares e com a ANPD, de forma clara e precisa e em língua portuguesa. A indicação deve levar em consideração seus conhecimentos sobre a legislação de proteção de dados pessoais, bem como o contexto, o volume e o risco das operações de tratamento realizadas. Tem as seguintes funções:

- conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis;
- apoiar o Gestor de Tecnologia da Informação e Comunicação, o Gestor de Segurança da Informação, juntamente com os proprietários de ativos, gestores do negócio ou de políticas públicas com orientações acerca das diretrizes que envolvam privacidade e proteção de dados pessoais nos termos do art. 41 da LGPD;
- havendo exfiltração de dados pessoais, informar à Autoridade Nacional de Proteção de Dados (ANPD) de acordo com os procedimentos previstos em legislação, normativos e orientações;
- aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações da autoridade nacional e adotar providências, orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as

demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares;

- Ser indicado por ato formal do agente de tratamento, do qual constem as formas de atuação e as atividades a serem desempenhadas;
- Ter um substituto formalmente designado para exercer suas funções nas ausências, impedimentos e vacâncias;
- Ser indicado pelo controlador e ter suas informações de identidade e contato divulgadas publicamente, de forma clara e objetiva, em local de destaque e de fácil acesso, no sítio eletrônico do agente de tratamento (no mínimo o nome completo, se for pessoa natural; ou o nome empresarial ou o título do estabelecimento, bem como o nome completo da pessoa natural responsável, se pessoa jurídica;
- Ter os meios necessários para o exercício de suas atribuições, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos;
- Receber solicitações de assistência e orientação por parte da empresa quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais;
- Ter garantia de autonomia técnica necessária para cumprir suas atividades, livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Ter garantido o acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização;
- orientar os funcionários e os contratados do agente de tratamento a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares;
- Ao receber comunicações da ANPD, adotar as medidas necessárias para o atendimento da solicitação e para o fornecimento das informações pertinentes, adotando, entre outras, encaminhar internamente a demanda para as unidades

competentes; fornecer a orientação e a assistência necessárias ao agente de tratamento; e indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado;

- prestar assistência e orientação ao agente de tratamento na elaboração, definição e implementação, conforme ocaso, de: registro e comunicação de incidente de segurança; registro das operações de tratamento de dados pessoais; relatório de impacto à proteção de dados pessoais; mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento dedados pessoais; medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito; processos e políticas internas que assegurem o cumprimento da Lei nº 13.709, de 14 de agosto de 2018, e dos regulamentos e orientações da ANPD; instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais; transferências internacionais de dados; regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da Lei nº 13.709, de 14 de agosto de 2018; produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais;
- atuar com ética, integridade e autonomia técnica, evitando situações que possam configurar conflito de interesse;
- Realizar a comunicação de incidente de segurança em nome do controlador, acompanhada de documento comprobatório de vínculo contratual, empregatício ou funcional, ou por meio de representante constituído, acompanhada de instrumento com poderes de representação junto à ANPD;

ANEXOS

ANEXO I- CONTEÚDO PROGRAMÁTICO DAS CAPACITAÇÕES E CONSCIENTIZAÇÕES DE SI&P

A tabela a seguir contempla a lista de temas que fazem parte do conteúdo programático das capacitações e conscientizações de SI&P da Companhia. A partir da segunda coluna, são apresentados os perfis, conforme tabela na seção "Perfis a serem Capacitados e Conscientizados" e, onde há preenchimento em verde, indica-se os temas das capacitações e conscientizações das quais cada um deve fazer parte.

Os tipos de capacitação e conscientização são os seguintes:

I. Especialização [ESP]: Requerem aprofundamento, podendo ser atendidos a partir de um conjunto de cursos e, quando cabível, certificação.
II. Fundamentos [FUND]: Requerem cursos de mercado que apresentam os conceitos iniciais sobre o assunto.
III. Conscientização Básica [CONS]: Capacitação personalizada, produzida pela própria Companhia.

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Gestão da Segurança da Informação & Privacidade e Comunicações • Gestão de Segurança da Informação e Comunicações • Normas de SI&P (ISO 27001, 27002,27701) • Governança • Leis, Regulação e Conformidade	ESP						

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Auditoria/Conformidade • Planejamento • Norma de auditoria de Sistema de Gestão ISO 19011 • Análise dos Riscos • Execução • Relatório Final	ESP						
Gestão de Continuidade de Negócios • Gestão de Continuidade de Negócios e Recuperação de Desastres • Norma ISO 22301 • Estratégias de Gestão de Continuidade de Negócios • Implementação, Manutenção e Testes • Cultura da Gestão de Continuidade de Negócios	ESP	FUND	FUND				
Gestão de Riscos • Planejamento de Gestão de Riscos • Normas de Riscos em SI&P ISO 27005, e Riscos ISO 31000) • Metodologias de Gestão de Riscos • Identificação de Riscos • Análise/Avaliação de Riscos • Tratamento de Riscos	ESP	FUND					

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Tratamento de Incidentes de Segurança Computacional/Gestão de Serviços • ITIL • Aspectos Normativos: criação de CSIRTS, CSIRTS de Governo; CSIRTS na Rede Mundial de Computadores • Processos de Monitoramento e Detecção de Intrusão • Processos de Análise e Resposta a Incidentes • Processos de Divulgação e Comunicação com Entidades Externas		ESP	FUND				
Forense Computacional • Aspectos Normativos • Técnicas de Cópia e Preservação de Evidências • Técnicas de Análise Forense		ESP					
Segurança no Desenvolvimento de Software • Vulnerabilidades de Software • Testes de Vulnerabilidade • Arquitetura de Software Seguro • Desenvolvimento Seguro • Codificação de Software Seguro/Desenvolvimento Seguro • OWASP (Projeto Aberto de Segurança em Aplicações Web) • Firewall de Aplicações Web				ESP			

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Controle de Acesso • Controle de acesso (senhas seguras, gerenciadores de senha, fatores de autenticação)		ESP		FUND			
Certificação Digital • Criptografia • Conceitos e Recursos • Convenções, Políticas e Formatos • Aplicações em uso • Assinatura Digital		ESP		FUND		CONS	
Fundamentos para Segurança da Informação • conceitos básicos de segurança da informação; • segurança física de ativos de informação; • segurança da informação em meio físico; e • classificação da informação o mesa limpa e como tratar informações classificadas o evitar exposição não intencional de dados (vazamento)						CONS	CONS
Fundamentos para Segurança Cibernética • conceitos básicos de segurança cibernética; • uso seguro da internet; e • uso seguro de aplicativos e outras ferramentas digitais;						CONS	CONS

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Segurança de Redes • Firewall • IDS/IPS • Arquiteturas e Escopo de Segurança • Segmentação • Tunelamento de Tráfego e VPN • Ethical Hacking • Frameworks NIST e CIS		ESP	FUND			CONS	CONS
Segurança de Redes – uso comum • Segurança de Aplicações e Serviços • Segurança Redes Wireless e Serviços Móveis • Segurança dos Dispositivos de Rede • Perigos de conectar e transmitir dados em redes inseguras; Perigos de conectar e transmitir dados em redes inseguras; • Como aumentar a segurança da rede caseiras em home office						CONS	CONS

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Segurança de Usuários • autenticação no acesso a sistemas e a serviços; • proteção de contas pessoais; • segurança em mídias sociais – aspectos técnicos; • segurança no uso de e-mail e outros aplicativos de comunicação; • segurança no uso de comércio eletrônico (e-commerce); • segurança no armazenamento e no compartilhamento de dados; • cópias de segurança de arquivos (backup); • segurança de dados em viagens; e • qualidade de vida digital; • proteção contra-ataques de engenharia social (Phishing, Pretexto, Isca, Quiproquó, Carona)						CONS	CONS
Computação em Nuvem • Conceitos Básicos • Modelos de Computação em Nuvem • Riscos da Computação em Nuvem • Proteção dos Dados • Responsabilidades dos Usuários • Responsabilidades do Provedor de Serviço	FUND	ESP	FUND	FUND		CONS	CONS

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS
Mobilidade • Conceito e Evolução • Riscos de Segurança associados com os Dispositivos Móveis • Segurança para Dispositivos Móveis • Gerenciamento de Dispositivos Móveis • Responsabilidades dos Usuários						CONS	CONS
Redes Sociais • Conceito e Evolução • Riscos de Segurança associados com o uso das Redes Sociais • Privacidade, Exposição e Comportamento do Usuário • Principais Controles de Segurança			ESP			CONS	
Direito Digital • conceitos jurídicos e legislação relacionados à segurança da informação; • direitos autorais; • assédio virtual; • fraudes e crimes na internet; • crimes cibernéticos.	FUND				ESP	CONS	

TEMA E CONTEÚDO RECOMENDADO	SI&P E GOV	CYBER E INFRA	SUPORTE	DESENV	JURÍDICO	COLABORADORES E PRESTADORES	USUÁRIOS

Incidentes de Segurança
• Reconhecimento e notificação de incidentes
• Principais vetores de ataques
• Identificar o tipo e a magnitude do problema
• Canais e meios de notificação
• Notificar falta de atualizações de Segurança
  ○ Verificar versão de software
  ○ Reconhecer mensagens de erro e log de processos automatizados
  ○ Informar a TI em caso de ocorrências
		ESP	FUND			CONS	CONS

ANEXO II – OBJETIVOS DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (SGPI)

	Objetivo	KPI	Descrição	Fórmula	Meta	Periodicidade	Responsável
1	Proteger os dados, dispositivos e sistemas de acesso contra acesso não autorizado e ameaças cibernéticas.	Percentual de sistemas com logs de acesso e transações implementados.	Mede o percentual de sistemas que possuem logs de acesso e transações implementados	(Sistemas com logs implementados / Total de sistemas) * 100	100%	Semestral	GEDES
2	Proteger os dados, dispositivos e sistemas de acesso contra acesso não autorizado e ameaças cibernéticas.	Percentual das CVEs aplicáveis a APS que foram tratadas	Mede o percentual das Vulnerabilidades “on the wild” aplicáveis a APS que foram tratadas, tanto por parte de um fabricante como pela APS.	(qtd CVEs tratadas/total de CVEs aplicáveis à APS) * 100	90%	Mensal	GERID
3	Garantir a confidencialidade, integridade e disponibilidade das informações	Percentual de Dispositivos com Definições de Antivírus Atualizados	Monitora a porcentagem de dispositivos que estão com os antivírus atualizados. Este é um indicador crítico para prevenir vulnerabilidades exploráveis.	(Dispositivos com antivírus atualizados / Total de dispositivos) x 100	90%	Mensal	GERID
4	Garantir a confidencialidade, integridade e disponibilidade das informações	Percentual de Backups Bem-Sucedidos	Monitora a porcentagem de tentativas de backup que foram completadas com sucesso sem erros, refletindo a confiabilidade das práticas de backup de dados.	(Número de backups bem-sucedidos / Total de tentativas de backup) x 100	95%	Mensal	GERID

5	Garantir a confidencialidade, integridade e disponibilidade das informações	Percentual de teste de restore Bem-Sucedidos	Monitora a porcentagem de tentativas de teste de restore que foram completadas com sucesso sem erros, refletindo a confiabilidade das práticas de backup de dados.	(Número de teste de restore de backups bem-sucedidos / Total de tentativas de teste de restore de backup) x 100	100%	Mensal	GERID
6	Garantir a confidencialidade, integridade e disponibilidade das informações	Nível de satisfação do cliente com a segurança dos dados fornecidos.	Monitora o nível de satisfação.	(Número de avaliações positivas / Total de avaliações recebidas) * 100	80%	Anual	SEGTI
7	Instruir empregados, estagiários e aprendizes sobre práticas de SI&P	Taxa de Participação nos Treinamentos de Segurança	Mede a porcentagem média de empregados que participaram nos treinamentos de segurança. Este KPI ajuda a verificar se todos os funcionários estão sendo adequadamente instruídos sobre as práticas de segurança.	(qtd média Participantes nos treinamentos de segurança / Total de empregados) x 100	80%	Anual	GECAR
8	Instruir empregados, estagiários e aprendizes sobre práticas de SI&P	Feedback dos Participantes sobre Treinamentos	Analisa as avaliações e comentários feitos pelos empregados sobre a utilidade dos treinamentos de segurança.	Média dos níveis de utilidade dos treinamentos	80%	Anual	GECAR
9	Instruir empregados, estagiários e aprendizes sobre práticas de SI&P	Feedback dos Participantes sobre Treinamentos	Analisa as avaliações e comentários feitos pelos empregados sobre a qualidade dos treinamentos de segurança.	Média dos níveis de qualidade dos treinamentos	80%	Anual	GECAR

10	Garantir a conformidades com Leis e Regulamentos de SI&P	Taxa de adequação com o Decreto Lei 9637	Monitora o nível de adequação com o Decreto Lei 9637. São considerados apenas os artigos da Lei aplicáveis à APS.	(Quantidade de itens largamente adequado + totalmente adequado + Preparado, não necessário) / total de itens a serem adequados	95%	Anual	SEGTI
11	Garantir a conformidades com Leis e Regulamentos de SI&P	Taxa de adequação com a LGPD	Monitora o nível de adequação com o LGPD. São considerados apenas os artigos da Lei aplicáveis à APS.	(Quantidade de itens largamente adequado + totalmente adequado + Preparado, não necessário) / total de itens a serem adequados	95%	Anual	SEGTI

Anexo III - Tratamento de Dados Pessoais

Este Anexo visa exemplificar e orientar a aplicação nos Termos de Referência de itens relativos ao tratamento de dados pessoais. Parte das diretrizes de segurança da informação e de privacidade já são observados através da aplicação de clausulas padrão nos contratos, porém em contratações que envolvem dados pessoais em seu escopo, há pontos que dependem de cada contrato, e devem ser elencados no TR (conforme modelo disponível) no item “SEGURANÇA DA INFORMAÇÃO E LGPD”.

Exemplo:

a) Nos termos da LGPD, nesse instrumento, a APS é identificada como (escolher uma das opções) Controladora/Operadora/Controladora Conjunta e a empresa contratada, como (escolher uma das opções) Controladora/Operadora/Controladora Conjunta.

b) Dados objetos do escopo do contrato, ações de tratamento e medidas de segurança.

Obs. 1) Se a empresa a ser contratada for enquadrada como “Operadora”, a APS é “Controladora” e vice-versa.

2) Quando a APS for considerada “Controladora Conjunta” a contratada também o é.

Conjunto de dados 1	
Dado, ou grupo de dados	Nome
Finalidade	Emissão de cartão, controle de utilização e saldo financeiro
Instrução para tratamento	Usar somente para o propósito especificado no contrato. Após o uso, os nomes devem ser anonimizados ou excluídos conforme as políticas de retenção
Uso Permitido	Envio de Mensagens personalizadas
Restrição	Não usar para marketing e nem compartilhar sem o consentimento
Medidas de segurança	Armazenamento criptografado, Transferência via protocolo seguro
Conjunto de dados 2	
Dado, ou grupo de dados	E-mail

Finalidade	Emissão de cartão, controle de utilização e saldo financeiro, acesso a APP de controle
Instrução para tratamento	Utilizar exclusivamente para os fins especificados e de acordo com o consentimento do titular. Manter segurança durante o armazenamento e transmissão.
Uso Permitido	Envio de comunicações relacionadas ao contrato; Envio de mensagens personalizadas
Restrição	Sem restrição
Medidas de segurança	Proteção contra divulgação

INFORMAÇÕES DE CONTROLE

TÍTULO

MANUAL SGPI - SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE (SI&P)

VERSÃO

4.0

UNIDADE GESTORA DO DOCUMENTO

SUPTI/SEGTI

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

ALTERAÇÕES NOS SEGUINTES ITENS DO DOCUMENTO:

- INCLUSÃO DE NOVAS DEFINIÇÕES
- INCLUSÃO E ALTERAÇÃO DE REFERENCIAIS LEGAIS
- INCLUSÃO DE NOVOS ITENS:
    - 6.8.4 COMPUTAÇÃO EM NUVEM
    - 7.7 TRANSFERÊNCIA INTERNACIONAL
    - 8.2 DEFINIÇÕES E FUNÇÕES DO ENCARREGADO E DO GESTOR DE SI.
- ALTERAÇÃO DO ITEM 6.7 PARA COMPARTILHAMENTO, TRANSFERENCIA E DIVULGAÇÃO DE DADOS E DE DADOS PESSOAIS

RELAÇÃO COM OUTROS NORMATIVOS

POLÍTICA DE SEGURANÇA E PRIVACIDADE.

NORMATIVOS REVOGADOS

INSTRUMENTO NORMATIVO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO: SEGURANÇA NAS OPERAÇÕES;

INSTRUMENTO NORMATIVO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO: SEGURANÇA NAS COMUNICAÇÕES;

INSTRUMENTO NORMATIVO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO: CRIPTOGRAFIA;

INSTRUMENTO NORMATIVO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO: SEGURANÇA FÍSICA E AMBIENTE;

INSTRUMENTO NORMATIVO SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO: PRIVACIDADE POR DESENHO E POR PADRÃO, ANONIMIZAÇÃO E PSEUDOMINIZAÇÃO.

INSTÂNCIA DE APROVAÇÃO

PRESIDENTE DA AUTORIDADE PORTUÁRIA DE SANTOS (APS) EM 08/12/2025, POR MEIO DO DOCUMENTO VIRTUAL N.º 46717/2022.