POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DA AUTORIDADE PORTUÁRIA DE SANTOS S.A.

CAPÍTULO I – DISPOSIÇÕES INICIAIS

1. Fica instituída a Política de Segurança da Informação e Privacidade da Autoridade Portuária de Santos S.A. ("***Autoridade Portuária de Santos***", "**APS**" ou "**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. A presente política orienta quanto a:

I. Garantir a segurança das informações e a proteção dos dados pessoais dos empregados e seus dependentes, prestadores de serviços e clientes.

II. 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.

III. 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, com foco na melhoria contínua dos processos e nas práticas de segurança.

SEÇÃO I – OBJETIVOS DA POLÍTICA

3. A presente Política de Segurança da Informação e Privacidade **("Política")** tem por objetivo estabelecer os princípios que orientam a Companhia, seus administradores, empregados, fornecedores e demais atores que desempenham atividades na e para a APS na preservação da confiabilidade das informações e

garantia da privacidade no tratamento de dados pessoais alinhada às exigências legais e às melhores práticas de segurança da informação e proteção de dados pessoais. Representa também o comprometimento com a preservação da segurança das informações e privacidade, em praticar esforços razoáveis e cumprimento dos requerimentos exigidos pela Lei para proteger a confidencialidade, integridade e disponibilidade das informações criadas, processadas, armazenadas e transmitidas como parte das suas atividades, bem como à privacidade.

4. Padronizar as práticas a serem aplicadas por todo o pessoal com responsabilidade para a segurança da informação e privacidade;

5. Dar consciência dos riscos que ameaçam o sistema de informação e os meios disponíveis para controlá-los;

6. Criar uma estrutura geral para projetar e executar medidas de segurança dos sistemas de informação; e

7. Promover a cooperação entre os departamentos da APS para criar, aplicar e verificar as instruções, procedimentos e medidas de segurança relacionadas ao negócio.

SEÇÃO II – ABRANGÊNCIA

8. A presente Política aplica-se aos empregados, estagiários, aprendizes membros dos órgãos estatutários da Companhia e suas filiais, prestadores de serviço (no desempenho de suas atividades em cumprimento de contratos e outros acordos semelhantes, principalmente nas atividades de tratamento de dados pessoais em que a APS figura como Controladora).

9. A Política de Segurança da Informação abrange a Defesa Cibernética, que tem como objetivo proteger a integridade, confidencialidade e disponibilidade das informações da Companhia contra ameaças cibernéticas.

SEÇÃO III – FUNDAMENTAÇÃO LEGAL E NORMATIVA

10. A Política de Segurança da Informação e Privacidade tem como fundamentação legal e normativa:

I. Estatuto Social da Companhia.

II. Resolução CGPAR Nº 41 de 4 de agosto de 2022, que estabelece diretrizes e parâmetros para implementação, desenvolvimento e aperfeiçoamento da Governança de Tecnologia da Informação e Comunicação nas empresas estatais federais.

III. ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements (Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação - Requisitos).

IV. 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).

V. 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).

VI. COBIT 5 Modelo Corporativo para Governança e Gestão de TI da Organização.

VII. ACÓRDÃO Nº 1016/2014 – TCU – Plenário, que recomenda que a APS institua práticas de segurança da informação.

VIII. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 (alterada pela Instrução Normativa Nº 2, de 24 de julho de 2020), que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal (GSI).

IX. Decreto nº 12.572/2025, de 04 de agosto de 2025 que Institui a Política Nacional de Segurança da Informação, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação no País.

X. Lei Federal nº 12.527 de 18/11/2011, Lei de Acesso à Informação.

XI. Lei Federal nº 12.965, de 23/04/2014, Marco Civil da Internet.

XII. Lei Federal nº 13.709 de 14/08/2018, Lei Geral de Proteção de Dados.

XIII. Guia Orientativo Para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, publicado pela ANPD versão de maio de 2021.

SEÇÃO IV – DEFINIÇÕES

11. Para os fins desta Política são adotadas as seguintes definições, que poderão ser utilizadas no singular ou plural, sem prejuízo de significado aqui atribuído, e que estão em conformidade com a legislação, com as adaptações necessárias à realidade da APS:

I. **Ativos de Informação:** Meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

II. **Comitê de Segurança da Informação e Privacidade (CSI):** Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e privacidade no âmbito do órgão ou entidade da administração pública federal;

III. **Confidencialidade:** diz respeito à divulgação não autorizada de informação sensível para o negócio;

IV. **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

V. **Controlador conjunto:** Duas ou mais entidades que, em conjunto, decidem as finalidades e os meios do tratamento de dados pessoais, sendo ambas responsáveis por garantir a conformidade com a legislação de proteção de dados;

VI. **Dados Pessoais:** Informação relacionada à pessoa natural identificada ou identificável;

VII. **Decisão Automatizada:** No âmbito das legislações de privacidade, trata-se de avaliações automatizadas de aspectos pessoais de uma pessoa, sem interferência humana, para que, com base nessa avaliação, sejam tomadas decisões, como definição de perfil, aprovação, rejeição, entre outras, que podem beneficiar ou prejudicar a pessoa;

VIII. **Disponibilidade:** relaciona-se à informação estar disponível quando requerido pelo processo de negócio agora e no futuro;

IX. **DPO – Data Protection Officer**: Vide Encarregado pelo Tratamento de Dados Pessoais;

X. **Encarregado pelo Tratamento de Dados Pessoais (Data Protection Officer - DPO):** Pessoa indicada pelo controlador, para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), dentre várias atribuições (Vide Capítulo Responsabilidades);

XI. **Indicador de Gestão:** um valor utilizado para avaliar o desempenho de um sistema, processo ou empresa. É orientado a dados e/ou métricas;

XII. **Integridade:** relaciona-se a exatidão, integralidade e autenticidade da informação, bem como a seu valor de acordo com os valores e expectativas da Companhia;

XIII. **Inteligência Artificial (IA):** um componente de um ou vários softwares utilizando técnicas de aprendizado (aprendizado de máquina e/ou aprendizado profundo), processamento de linguagem natural para gerar resultados baseados nos dados utilizados no aprendizado, via linguagem natural ou outros meios de interação, inclusive com outros componentes de IA;

XIV. **KPI:** Sigla de *Key Perfomance Indicator*, ou Indicador-Chave de Desempenho, é uma medida quantitativa usada para avaliar o progresso de uma empresa em direção a metas específicas;

XV. **Operador:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

XVI. **Privacidade:** diz respeito à proteção dos dados pessoais, incluindo o respeito, liberdade e as garantias constitucionais do cidadão;

XVII. **SGPI:** Sigla de Sistema de Gestão da Segurança da Informação e Privacidade;

XVIII. **Sistema de Gestão da Segurança da Informação, e Privacidade**: Consiste em políticas, procedimentos, guias e outros recursos e atividades associados que são coletivamente gerenciados por uma organização na busca pela proteção de seus ativos de informação, sob a ótica da Segurança da Informação e Privacidade;

XIX. **Segurança da Informação (SI):** Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XX. **Sistema de Inteligência Artificial (IA):** é um software projetado para replicar capacidades humanas, como aprendizado, raciocínio lógico, reconhecimento de padrões e interação em linguagem natural;

XXI. **Tecnologia da Informação e Comunicação (TIC):** Conjunto de conhecimentos, sistemas, processos e práticas utilizadas na prestação de serviços de suporte aos processos empresariais de quaisquer naturezas, através de captura, processamento, geração, armazenamento, recuperação e comunicação de dados, informações e conhecimentos;

XXII. **Titulares dos Dados Pessoais:** Pessoa natural a quem se referem os dados pessoais objeto de tratamento;

XXIII. **Tratamento de Dados Pessoais:** Toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

XXIV. **Violações de Dados Pessoais:** Quebra de segurança (acidental ou proposital) que resulte na destruição, perda, alteração, divulgação não autorizada de, ou acesso não autorizado a dados pessoais transmitidos, armazenados ou de outra forma tratados, incluindo acesso ilegal, vazamento ou perda de dados pessoais em função de ataques cibernéticos, erro humano, roubo ou perda de dispositivos contendo dados pessoais.

CAPÍTULO II – PRINCÍPIOS

12. São princípios da APS em relação à Segurança da Informação e Privacidade:

I. Garantir a confiabilidade das informações, através de critérios de confidencialidade, integridade, disponibilidade e autenticidade das informações;

II. Garantir a privacidade através do tratamento adequado dos dados pessoais de acordo com legislações pertinentes e as boas práticas.

13. São princípios da APS em relação à proteção de dados pessoais:

I. **Licitude, Lealdade e Transparência:** O tratamento dos dados pessoais somente poderá ser realizado de forma lícita, leal, justa e transparente em relação à observância as normas de proteção de dados ao titular dos dados, inclusive quando envolver a utilização de sistemas de Inteligência Artificial.

II. **Limitação de Finalidade:** Os dados pessoais somente poderão ser tratados (utilizando qualquer meio, inclusive sistema de Inteligência Artificial) para finalidades explícitas, não discriminatórias, legítimas e especificadas, não sendo posteriormente tratados de maneira incompatível com essas finalidades.

III. **Minimização dos Dados:** Somente poderão ser coletados de forma adequada dados pessoais que sejam pertinentes, limitados e necessários às finalidades e objetivos para as quais são processados.

IV. **Exatidão ou Precisão:** Os dados pessoais devem ser exatos e mantidos atualizados sempre que necessário. Devem ser adotadas medidas para garantir que dados inexatos sejam corrigidos ou excluídos sem demora.

V. **Limitação de Retenção ou conservação:** Os dados pessoais devem ser mantidos apenas pelo período necessário para a consecução das finalidades a que se destinam.

VI. **Integridade e Confidencialidade:** Os dados pessoais deverão ser tratados de maneira a garantir sua segurança, proteção, acesso não autorizado ou ilícito, de forma a evitar a perda, destruição ou dano proposital ou acidental.

CAPÍTULO III – DIRETRIZES

SEÇÃO I – DIRETRIZES GERAIS

14. Os controles de segurança da informação e privacidade devem ser baseados em uma avaliação de riscos, incorporando medidas organizacionais, técnicas e físicas, além de respeitar as melhores práticas e legislações relevantes;

15. Os controles de segurança de segurança da informação e privacidade devem ser normatizados, os quais passam a complementar a presente política;

16. Os controles de segurança da informação e privacidade devem incluir, no mínimo, os seguintes aspectos:

I. Tratamento da Informação (classificação da informação, uso e processamento, armazenamento e transmissão):

a) Todas as informações devem ser classificadas conforme sua criticidade e sensibilidade, com base em uma Classificação da Informação;

b) Dados sensíveis e críticos devem ser protegidos por meio de criptografia durante o armazenamento (em repouso) e a transmissão (em trânsito), utilizando algoritmos reconhecidos e de boa prática, como AES-256;

c) Chaves criptográficas devem ser gerenciadas adequadamente, incluindo geração, distribuição, armazenamento, uso e descarte seguro, conforme os padrões definidos na Gestão de Chaves Criptográficas.

II. Segurança Física e do Ambiente:

a) As áreas críticas, como datacenters, devem ser protegidas contra incêndios, falhas de energia e outras ameaças ambientais, por meio

de sistemas como: Detectores de fumaça e calor; Sistema de combate a incêndios, preferencialmente com supressores adequados para equipamentos eletrônicos;

b) Proteção contra quedas e surtos de energia, com uso de *no-breaks* (UPS) e geradores de backup;

c) Deve ser garantido que todos os equipamentos e instalações estejam em conformidade com as normas de proteção ambiental e de segurança contra incêndios locais;

d) O acesso às áreas sensíveis e restritas, como data centers, salas de servidores, áreas de TI e armazenamento de documentos confidenciais, deve ser controlado por credenciais eletrônicas, cartões de acesso ou biometria;

e) O princípio do menor privilégio deve ser seguido para conceder acesso físico. Apenas pessoal autorizado, cujas funções requerem presença nestas áreas, devem receber credenciais de acesso; Registros de acesso físico (logs) devem ser mantidos e revisados periodicamente para identificar possíveis acessos não autorizados ou anômalos.

III. Gestão de Incidentes de Segurança da Informação:

a) Incidentes de segurança devem ser reportados imediatamente à equipe de segurança da informação por meio dos canais designados;

b) Um plano de resposta a incidentes deve ser mantido e testado regularmente para garantir que todos os envolvidos estejam preparados para lidar com falhas de segurança, minimizando o impacto à organização;

c) Todos os incidentes devem ser registrados, investigados e as medidas corretivas aplicadas para evitar reincidência.

IV. Gestão de Ativos:

a) Todos os ativos de informação da Companhia, incluindo hardware, software, dados e documentos, devem ser inventariados e classificados de acordo com seu valor, criticidade e sensibilidade. Cada ativo deve ter um responsável designado, que será encarregado de garantir sua proteção e uso adequado;

b) O inventário de ativos deve ser atualizado regularmente, e qualquer movimentação ou descarte de ativos deve ser devidamente registrada e controlada, garantindo que dados sensíveis sejam eliminados de forma segura;

c) O uso aceitável de ativos deve ser implementado, abrangendo desde o acesso até o descarte, com regras específicas para a utilização de dispositivos móveis e recursos de TI.

V. Gestão do Uso dos Recursos Operacionais e de Comunicações, como: e-mail, acesso à internet, mídias sociais, computação em nuvem, dentre outros:

a) Os recursos operacionais e de comunicação, como e-mails, internet, mídias sociais e plataformas de computação em nuvem, devem ser usados exclusivamente para fins profissionais, respeitando as políticas internas de segurança e conformidade. O acesso a esses recursos deve ser monitorado, e todos os colaboradores devem utilizar autenticação segura e práticas recomendadas para proteger informações confidenciais. O uso de e-mails e mídias sociais para compartilhar dados sensíveis é estritamente proibido sem as devidas precauções de segurança, como criptografia.

VI. Controles de Acesso:

a) O acesso às informações e sistemas deve ser concedido com base no princípio do menor privilégio. Os usuários devem ter apenas os acessos necessários para desempenhar suas funções.

VII. Gestão de Riscos:

a) Os riscos de segurança da informação devem ser identificados, avaliados e mitigados de forma contínua, garantindo que ameaças aos ativos e processos críticos sejam adequadamente controladas, através de um processo formal de gestão de riscos, incluindo análises periódicas para revisar potenciais vulnerabilidades e definir medidas corretivas. Todos os colaboradores são responsáveis por reportar qualquer incidente ou risco emergente, para que seja tratado de acordo com o plano de resposta a riscos.

b) Os riscos identificados devem ser documentados e priorizados com base em sua probabilidade e impacto, sendo monitorados regularmente para assegurar que os controles sejam eficazes. A mitigação de riscos deve ser feita considerando tanto medidas preventivas quanto reativas.

VIII. Gestão de Continuidade:

a) Um plano de continuidade de negócios e recuperação de desastres deve ser estabelecido para garantir a rápida recuperação de processos críticos em caso de interrupções. Este plano deve ser revisado e testado regularmente para assegurar sua eficácia e preparar a organização para enfrentar cenários de incidentes. As áreas e sistemas críticos devem ter medidas de contingência estabelecidas, como backups de dados e infraestrutura de recuperação em locais alternativos.

b) Deve haver procedimentos de continuidade de negócios, e responsabilidades específicas devem ser atribuídas para ações de resposta a crises. A gestão da continuidade deve estar integrada aos processos de gestão de risco e segurança da informação, visando minimizar impactos operacionais e preservar a integridade dos dados.

IX. Auditoria e Conformidade:

a) Auditorias periódicas para avaliar a conformidade com as políticas de segurança da informação, legislações aplicáveis e normas internas devem ser realizadas. Essas auditorias devem ser conduzidas de forma imparcial e documentada, com resultados que direcionem melhorias nos processos de segurança. As não conformidades identificadas devem ser tratadas com planos de ação corretivos, e as auditorias devem garantir que todas as áreas estejam aderentes aos requisitos regulatórios e de segurança.

b) Diretrizes de conformidade devem ser estabelecidas e seguidas, e qualquer desvio deve ser reportado e corrigido. A alta direção deve revisar os resultados das auditorias para garantir que a organização se mantenha em conformidade contínua com suas obrigações legais e padrões de governança.

17. Em relação ao tratamento de dados pessoais pela APS:

I. As atividades de tratamento de dados pessoais deverão ser executadas considerando:

a) Legitimidade

b) Transparência

c) Limitação ao uso dos dados estritamente necessários e não invasivos

d) Respeito à privacidade

e) Segurança e proteção aos dados pessoais

II. Deverá haver mecanismos para que os titulares dos dados pessoais possam exercer seus direitos conforme a Lei.

18. A Segurança da Informação e Privacidade deverá ser considerada em outras áreas de conhecimento complementando os respectivos aspectos inerentes, em especial nas disciplinas de:

I. Gestão de Projetos
II. Gestão de Continuidade
III. Uso de Inteligência Artificial, inclusive na utilização de ferramentas de IA próprias ou de terceiros

SEÇÃO II – DIRETRIZES DE PRIVACIDADE (OU PROTEÇÃO E TRATAMENTO DE DADOS PESSOAIS)

19. Como parte desta política, a APS estabelece as diretrizes para a proteção de dados pessoais para assegurar a confidencialidade, integridade e disponibilidade dos dados pessoais em conformidade e sob a ótica e termos da legislação de proteção de dados pessoais.

20. O tratamento de dados pessoais somente poderá ocorrer se observados os princípios, a boa-fé, e os requisitos para o tratamento de Dados Pessoais.

21. Os requisitos para o tratamento de Dados Pessoais e Dados Pessoais Sensíveis (inclusive de crianças e adolescentes) de acordo com a Lei, levam em consideração:

I. Hipóteses Legais (LGPD Art. 7º, Art. 11) que permitem e condicionam o tratamento.
II. Coleta e retirada de consentimento quando necessário (em especial quando envolver a utilização de sistemas de inteligência Artificial).
III. Os direitos dos titulares e as possibilidades de exercício desses direitos.
IV. A necessidade e condições para Transferência Internacional de dados pessoais.
V. A necessidade e condições para Compartilhamento de dados pessoais.
VI. O Legítimo Interesse da APS, se aplicável.

22. Os Agentes de tratamento de dados pessoais previstos no âmbito da APS, para a execução de atividades e de acordo com a LGPD, são:

I. Controlador
II. Operador
III. Controlador conjunto

23. Nas atividades de tratamento de dados pessoais em que a APS figurar como "Controladora", em consonância com as regulamentações aplicáveis deve:

I. Prover facilidades mínimas para receber e atender solicitações dos titulares de dados pessoais.
II. Solicitar do Encarregado assistência e orientações sobre as práticas em relação à proteção de dados pessoais.
III. Responsabilizar-se pela conformidade do tratamento de dados pessoais.
IV. Determinar, quando aplicável, as ações de tratamento de dados pessoais a serem executadas por empresas consideradas como "Operador".
V. Desempenhar outras ações previstas em regulamentações.

24. Nas atividades de tratamento de dados pessoais em que APS figurar como "Operadora", em consonância com as regulamentações aplicáveis deve:

I. Realizar as ações de tratamento de dados pessoais conforme determinado pelo "Controlador".
II. Comunicar imediatamente ao "Controlador" a ocorrência de incidentes de segurança envolvendo dados pessoais do "Controlador".
III. Desempenhar outras ações previstas em regulamentações.

25. Nas atividades de tratamento de dados pessoais em que APS figurar como "Controladora Conjunta", em consonância com as regulamentações aplicáveis deve:

I. Realizar as ações de tratamento de dados pessoais conforme descrito no tópico como "Controlador", e de acordo com o determinado em conjunto.
II. Desempenhar outras ações previstas em regulamentações.

26. Os titulares dos dados pessoais, resguardados as restrições legais, têm os seguintes direitos, inclusive quando envolver a utilização de sistemas de Inteligência Artificial:

I. **confirmação e acesso:** é direito do titular a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de acessar os seus dados pessoais;

II. **correção:** é direito do titular obter, sem demora injustificada, a correção dos dados pessoais inexatos que lhe digam respeito;

III. **anonimização, bloqueio ou eliminação:** é direito do titular de ter seus dados considerados desnecessários, excessivos ou tratados em desconformidade com a Lei;

IV. **portabilidade:** é direito do titular controlar, gerenciar e reutilizar seus dados pessoais, permitindo a transferência de suas informações para outra entidade;

V. **eliminação dos dados:** é direito do titular ter seus dados apagados ao término da finalidade específica do motivo da retenção ou conservação, ou tratadas com o seu consentimento, exceto nos casos previstos em Lei;

VI. **Informação sobre compartilhamento com entidades públicas e/ou privadas;**

VII. **Negação de consentimento:** é direito do titular, quando da solicitação de consentimento, negar o consentimento e conhecer as consequências da negativa;

VIII. **Revogação de consentimento:** é direito do titular retirar o consentimento dado anteriormente para uma atividade específica;

IX. **Revisão de decisões automatizadas:** é direito do titular solicitar uma revisão de decisões que foram tomadas de forma automática, especialmente quando essas decisões envolvem a criação de perfis com base em suas informações pessoais, inclusive se forem feitas por meio de Inteligência Artificial.

27. A APS manterá designado um Encarregado pela Proteção de Dados (vide itens Definições e Responsabilidade) parte do quadro da APS ou contratado especificamente para essa função, conforme regulamentação aplicável.

28. A APS seguirá os procedimentos definidos na legislação vigente, e pela Autoridade Nacional de Proteção de Dados (ANPD), no caso de violação de dados pessoais.

29. As características das atividades de tratamento de dados pessoais executadas na APS, deverão ser comunicadas através de "Termos de Privacidade" publicados nos sites conforme o público-alvo (interno e/ou externo), constando:

I. Os titulares;

II. As finalidades;

III. As categorias dos dados pessoais;

IV. Caso o público-alvo seja usuários intranet/internet através das páginas disponibilizadas, os cookies utilizados e suas finalidades devem ser claramente informados. Nesse caso, o site deverá disponibilizar um painel de cookies para permitir a habilitação ou desabilitação desses cookies;

V. Outras informações pertinentes e relativas ao tratamento de dados pessoais e de acordo com a legislação.

30. Os tratamentos de dados pessoais que envolvam o uso de recursos em outras jurisdições (países), caracterizando uma "transferência internacional", só poderão ocorrer em conformidade com a LGPD.

31. As atividades de tratamento de dados pessoais deverão ser documentadas e, quando aplicável, acompanhado de uma análise de risco com vistas a adoção de medidas de redução/eliminação de riscos (ou adequação da atividade) e elaboração de relatório de impacto à privacidade.

32. As atividades de tratamento de dados pessoais deverão ocorrer considerando os requisitos de segurança da informação, sem os quais não é possível

atingir os objetivos da proteção de dados pessoais (privacidade), aplicando as medidas técnicas e organizacionais aptas a também proteger os dados pessoais, contra acessos não autorizados, destruição, perda, alteração, comunicação ou difusão indevida de tais dados.

CAPÍTULO IV – RESPONSABILIDADES

SEÇÃO I – UNIDADES RESPONSÁVEIS

33. No âmbito da presente Política, as instâncias e unidades de gestão abaixo elencadas são responsáveis, além das suas respectivas atribuições previstas no Regimento Interno da Companhia, por:

I. Superintendência de Tecnologia da Informação (SUPTI):

a) Definir e Manter o SGPI, através da elaboração de normativos de SI&P, bem como instrução para apreciação e/ou aprovação pela instância de aprovação;

b) Manter o SGPI, através da viabilização das ações de redução ou mitigação de riscos de SI&P;

c) Manter o SGPI, através da viabilização das ações de melhoria contínua;

d) Estimular e/ou fomentar a aplicação das diretrizes desta Política e dos normativos do SGPI nas áreas da Companhia.

II. COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

a) O Comitê de Segurança da Informação (CSI) deve coordenar as atividades de Segurança da Informação em toda a Companhia. Seu funcionamento deve estar estabelecido por um Regimento Interno.

III. DIRETORIA EXECUTIVA (DIREXE)

a) Garantir o atendimento das políticas de Segurança da Informação e o funcionamento do SGPI;

b) Garantir a compatibilidade da segurança da informação com os objetivos estratégicos da Companhia;
c) Aprovar as iniciativas para a melhoria contínua do SGPI;
d) Prover recursos para a gestão, operação e monitoramento adequado das atividades do SGPI;
e) Suportar perante toda a Companhia as iniciativas da Área de Segurança da Informação;
f) Garantir a contínua manutenção das Políticas de Segurança da Informação e desdobramento de seus respectivos objetivos;
g) Garantir a contínua análise e realimentação dos resultados de gestão de riscos ao SGPI;
h) Ter conhecimento das auditorias conduzidas no sistema de gestão para que os planos de ação sejam cumpridos.

IV. GESTOR DE SEGURANÇA DA INFORMAÇÃO

a) Produzir diretivas locais de segurança, regras e padrões a serem usados pelos empregados;
b) Propor recursos necessários às ações de segurança da informação e comunicações;
c) Coordenar o Comitê de Segurança da Informação e Comunicações - CSI;
d) Desenvolver e promover programas de conscientização de segurança;
e) Garantir que todos os gestores estejam cientes de suas próprias responsabilidades relacionadas à Segurança da Informação;
f) Manter-se atualizado com relação à tecnologia, legislação e novas ameaças;
g) Analisar criticamente os incidentes de segurança mais significativos e gerenciar e/ou acompanhar as ações relacionadas à solução deles;

h) Representar a Companhia externamente, mediante autorização e quando aplicável, nos assuntos relacionados ao SGPI;

i) Assessorar a direção na implementação da Política de Segurança da Informação e privacidade, considerando:

   1. O gerenciamento dos processos do SGPI, na busca da melhoria contínua;
   2. A coleta de dados e informações pertinentes à segurança da informação para a realização de análise crítica pela Direção;
   3. O fornecimento de resultados das análises críticas realizadas pela direção, aos envolvidos, visando providências;

j) Acompanhar o sistema de ações corretivas e preventivas do SGPI; e

k) Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação.

V. GESTORES das unidades funcionais da APS

a) Implantar e monitorar a eficácia de procedimentos, instruções de trabalho e documentos quanto a proteção da Segurança da Informação em sua área de atuação;

b) Informar/comunicar todos os fatos relacionados ao SGPI às áreas de operação sob sua responsabilidade;

c) Contribuir para implantação dos objetivos de gestão de Segurança da Informação e efetuar as medições necessárias por processos;

d) Implantar as oportunidades de melhoria;

e) Garantir a contínua eficácia dos controles implantados para satisfazer os requisitos do SGPI;

f) Solicitar assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

VI. EMPREGADOS e todos os funcionários, terceiros e prestadores de serviço com funções dentro da estrutura da APS.

a) Notificar seus gestores sobre qualquer alteração no inventário de ativos de sua área;
b) Conhecer e seguir os procedimentos pertencentes ao SGPI;
c) Recomendar melhorias no SGPI;
d) Identificar qualquer incidente de segurança e reportá-lo ao seu gestor/contato direto dentro da Companhia;
e) Cuidar pela proteção dos ativos de informação a que tiverem acesso.

VII. **PROPRIETÁRIOS DA INFORMAÇÃO:** Proprietários da Informação são Supervisores, Gerentes, Superintendentes e Diretores das unidades organizacionais que possuem responsabilidade primária por ativos de informação, associados com sua autoridade funcional, ou que estejam conduzindo projetos de TI que envolva o desenvolvimento, teste e liberação de aplicativos, sistemas etc.

a) Determinar os requerimentos de confidencialidade, integridade e disponibilidade para proteger esses ativos de informação relacionados com os processos de negócio ao seu cargo;
b) Definir procedimentos que suportem as políticas e procedimentos de Segurança da Informação;
c) Segregar funções e separar recursos de desenvolvimento, teste e produção dentro dos seus processos de negócio;
d) Gerenciar a correta prestação de serviços por parte de terceiros que afetem/suportem a segurança dos ativos de informação ao seu cargo, fazendo análise crítica do seu desempenho e possíveis oportunidades de melhoria;
e) Analisar criticamente em seus processos de negócio e em particular dos riscos à informação e privacidade.

VIII. **Encarregado pelo Tratamento de Dados Pessoais (DPO)**

a) Aceitar reclamações e comunicações dos titulares, prestando esclarecimentos e adotando as providências cabíveis;

b) Receber comunicações da ANPD e tomar as providências necessárias;
c) Orientar os funcionários e contratados sobre práticas de proteção de dados pessoais;
d) Atuar com ética, integridade e autonomia técnica, evitando conflitos de interesse;
e) Cabe, ainda, ao encarregado:
    I. Prestar assistência na elaboração e implementação de registros de incidentes de segurança e operações de tratamento de dados;
    II. Auxiliar na elaboração de relatórios de impacto à proteção de dados pessoais;
    III. Implementar mecanismos internos de supervisão e mitigação de riscos relacionados ao tratamento de dados pessoais;
    IV. Recomendar medidas de segurança para proteger os dados pessoais contra acessos não autorizados e situações ilícitas;
    V. Contribuir para processos e políticas que assegurem o cumprimento da LGPD e orientações da ANPD;
    VI. Auxiliar na elaboração de instrumentos contratuais relacionados ao tratamento de dados pessoais;
    VII. Apoiar na gestão de transferências internacionais de dados.
    VIII. Promover boas práticas e governança em privacidade, conforme estabelecido pela LGPD;
    IX. Colaborar no desenvolvimento de produtos e serviços com padrões de design que respeitem os princípios da LGPD;
    X. Prestar assistência e orientação em outras atividades e decisões estratégicas referentes ao tratamento de dados pessoais;
    XI. Declarar ao agente de tratamento qualquer situação que possa configurar conflito de interesse.

CAPÍTULO V – SANÇÕES

34. A não observância desta Política e de seus desdobramentos normativos implicará, no que couber, em sanções previstas no Regulamento Interno de Pessoal (RIP) e/ou no Código de Ética da APS e/ou no Manual de Conduta e Integridade da APS.

CAPÍTULO VI - DISPOSIÇÕES GERAIS

35. Compete aos gestores da Companhia difundir a presente Política e seus desdobramentos aos empregados e zelar por seu cumprimento.

36. É dever dos administradores e empregados da Companhia observar os princípios e procedimentos estabelecidos neste documento.

37. A presente política deve ser revista a qualquer momento em decorrência de eventual atualização na estratégia corporativa da APS, ou periodicamente, não podendo exceder em 4 (quatro) anos entre cada revisão.

38. As exceções à presente política serão avaliadas e devem ser reportadas por escrito ao Comitê de Segurança da Informação. Este irá avaliar as exceções conforme as justificativas de negócio fornecidas pelo solicitante e definir o tratamento adequado.

INFORMAÇÕES DE CONTROLE

TÍTULO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

VERSÃO

2.0

UNIDADE GESTORA DO DOCUMENTO

SUPERVISÃO DE GOVERNANÇA DE TI

ALTERAÇÕES EM RELAÇÃO À VERSÃO ANTERIOR

TRANSFERÊNCIA DOS ITENS COOKIES E CLASSIFICAÇÃO DA INFORMAÇÃO PARA O MANUAL SGPI.

TRANSFERÊNCIA DO ITEM SGPI PARA O NOVO MANUAL DO SISTEMA DE GESTÃO.

RELAÇÃO COM OUTROS NORMATIVOS

ESTATUTO SOCIAL

POL.SERCI.GCO.035 POLÍTICA DE GESTÃO DE CONTINUIDADE DO NEGÓCIO

INP TIC-020 GESTÃO DE SERVIÇOS DE TIC

INP TIC-110 GERIR PROCESSO DE SOFTWARE

INP-SUPTI-TIC-140-008-Gestão de Ativos

INP TIC-140-007 SISTEMA DE GESTÃO DA PRIVACIDADE DA INFORMAÇÃO: GESTÃO DE PESSOAS

MAN.SUPTI.TIC.003 MANUAL SGPI: USO ACEITÁVEL DE ATIVOS DE TIC

MAN.SUPTI.TIC.011 MANUAL SGPI - SEGURANÇA DA INFORMAÇÃO & PRIVACIDADE (SI&P)

MAN.SUGEP.RHU.007 MANUAL DE ORIENTAÇÕES AO TELETRABALHO

MAN.SUPTI.TIC.010 MANUAL SGPI - ANÁLISE E AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

MAN.SUCOC.TIC.008 MANUAL DE USO SEGURO DE MÍDIAS SOCIAIS

CARTILHA DE UTILIZAÇÃO DE RECURSOS COMPUTACIONAIS

MAN.GECOP.GCO.022 MANUAL DE CONDUTA E INTEGRIDADE

NORMATIVOS REVOGADOS

N/A

INSTÂNCIA DE APROVAÇÃO

CONSELHO DE ADMINISTRAÇÃO DA APS, 726ª REUNIÃO REALIZADA EM 25/09/2025, POR MEIO DA DELIBERAÇÃO CONSAD Nº 120.2025