1. OBJETIVO

O Instituto de Pesquisa Econômica e Previdência - IPEP define sua Política de Segurança da Informação e Privacidade ("PSIP") como documento normativo de nível estratégico e componente essencial do seu Sistema de Gestão de Segurança da Informação (SGSI) e do Sistema de Gestão de Privacidade da Informação (SGPI), estabelecidos em conformidade com os requisitos das normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019, com as melhores práticas definidas na ABNT NBR ISO/IEC 27002:2022, e com a legislação brasileira aplicável, em especial a Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018).

Seu objetivo é estabelecer os princípios, diretrizes e responsabilidades que assegurem proteção adequada às informações e dados pessoais tratados pelo IPEP, bem como os de seus clientes, colaboradores e demais partes interessadas, por meio de abordagem sistemática e baseada em riscos para a gestão da segurança da informação e da privacidade.

2. PROPÓSITO

Esta política busca definir diretrizes e normas de Segurança da Informação e Privacidade que possibilitem a todos os usuários e partes interessadas do IPEP adotarem comportamentos seguros e em conformidade com os requisitos do SGSI e do SGPI, bem como:

- Orientar sobre a implementação de controles e procedimentos para atender às exigências de Segurança da Informação e Privacidade dos Dados Pessoais;
- Proteger os dados do IPEP, assegurando os requisitos fundamentais de confidencialidade, integridade e disponibilidade;
- Evitar possíveis causas de incidentes e responsabilidades jurídicas da instituição, bem como de seus colaboradores, clientes, fornecedores e parceiros;
- Reduzir os riscos de perdas financeiras, de participação no mercado, da confiança dos clientes ou de quaisquer outros efeitos prejudiciais ao negócio do IPEP decorrentes de falhas de segurança;
- Assegurar a conformidade com as obrigações legais, regulatórias e contratuais aplicáveis, incluindo a LGPD, e atender aos requisitos das normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019;
- Fomentar a cultura de segurança da informação e privacidade por meio de programas contínuos de conscientização e capacitação;
- Promover a melhoria contínua do SGSI e do SGPI, por meio de monitoramento, medição, análise e avaliação sistemática de desempenho.

3. POLÍTICA

Esta política é válida para todos os colaboradores (efetivos, temporários, estagiários e aprendizes), prestadores de serviço, fornecedores e parceiros do IPEP que, em qualquer capacidade, tenham acesso a informações, dados pessoais, sistemas de informação, ambientes de tecnologia ou

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

demais ativos de informação do IPEP, independentemente do local de trabalho (presencial ou remoto) ou do meio de acesso utilizado.

O descumprimento desta Política é considerado infração grave e pode resultar nas medidas disciplinares descritas na Seção 5 deste documento.

3.1 POLÍTICA DO INSTITUTO DE PESQUISA ECONÔMICA E PREVIDÊNCIA – IPEP

- Desenvolver, implementar e monitorar integralmente políticas, normas e procedimentos de segurança da informação, assegurando que os requisitos fundamentais de confidencialidade, integridade e disponibilidade das informações e dados pessoais tratados no IPEP sejam cumpridos por meio da adoção de medidas de controle contra ameaças originadas de fontes internas e externas;
- Fornecer a todas as partes interessadas e autorizadas, como colaboradores, terceiros contratados, fornecedores e, quando aplicável, clientes, as políticas, normas e procedimentos de segurança.
- Assegurar que os Colaboradores, terceiros contratados, fornecedores e, quando aplicável, clientes estejam informados e conscientizados sobre as práticas de segurança da informação e privacidade de dados implementadas pelo IPEP.
- Cumprir integralmente os requisitos de segurança da informação e privacidade dos dados pessoais que são aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
- Gerenciar de forma abrangente os incidentes de segurança da informação e privacidade de dados pessoais, assegurando que sejam devidamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicados às autoridades competentes;
- Assegurar a continuidade das operações por meio da adoção, implementação, testes e aprimoramento constante de planos de continuidade e recuperação de desastres;
- Aprimorar constantemente a Gestão de Segurança da Informação e Privacidade por meio da definição e revisão sistemática dos objetivos de segurança em todas as instâncias da organização;
- Implementar e manter processo formal de avaliação e tratamento de riscos de segurança da informação e privacidade, assegurando que os riscos identificados sejam tratados com controles proporcionais ao seu nível de criticidade, em conformidade com os critérios definidos pelo CGSI;
- Assegurar que o tratamento de dados pessoais realizado pelo IPEP, na condição de controlador ou operador, ocorra estritamente de acordo com as bases legais e os princípios estabelecidos na LGPD, garantindo os direitos dos titulares de dados;
- Manter e testar regularmente planos de resposta a incidentes de segurança da informação e de violação de dados pessoais, assegurando notificação à Autoridade

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

Nacional de Proteção de Dados (ANPD) e aos titulares afetados, quando exigido pela LGPD;

- Assegurar que a segurança da informação e a privacidade sejam consideradas desde a concepção de novos produtos, serviços e sistemas, em conformidade com o art. 46, § 2º da LGPD e com os controles da ABNT NBR ISO/IEC 27002:2022.

4. PAPÉIS E RESPONSABILIDADES

4.1 ALTA DIREÇÃO

A Alta Direção do IPEP demonstra liderança e comprometimento com o SGSI e o SGPI, sendo responsável por:

i. Aprovar formalmente esta Política e os objetivos de segurança da informação e privacidade, garantindo seu alinhamento estratégico com os objetivos institucionais;
ii. Assegurar a disponibilidade dos recursos necessários para implementação e manutenção do SGSI e do SGPI;
iii. Conduzir a análise crítica periódica do SGSI e do SGPI para assegurar sua pertinência, adequação e eficácia; e
iv. Promover cultura organizacional que valorize a segurança da informação e a proteção de dados pessoais.

4.2 Comitê Gestor de Segurança da Informação – CGSI

É estabelecido o Comitê Gestor de Segurança da Informação - CGSI, com a presença de, no mínimo: um DPO, um Diretor de Compliance e Risco e dois integrantes com expertise em tecnologia da informação, seja no suporte à infraestrutura ou no desenvolvimento de sistemas.

É responsabilidade do CGSI:

i. Examinar, revisar e sugerir a aprovação de diretrizes e normas vinculadas à segurança da informação;
ii. Assegurar a disponibilidade dos recursos essenciais para uma Gestão de Segurança da Informação eficaz;
i. Acompanhar e avaliar a gestão de riscos de segurança da informação;
ii. Avaliação de risco antes de cada nova contratação de Plataformas e / ou IA;
iii. Deliberar sobre incidentes relevantes de segurança da informação e as ações corretivas;
iv. Garantir que as atividades de segurança da informação e privacidade de dados sejam executadas em conformidade com a PSIP;
v. Promover a divulgação da PSIP e tomar ações necessárias para disseminar uma cultura de segurança da informação e de privacidade de dados pessoais no ambiente da organização;
vi. Coordenar o processo de avaliação de riscos de segurança da informação e privacidade, aprovando os critérios de aceitação de risco e os planos de tratamento;
vii. Aprovar e revisar periodicamente o Plano de Tratamento de Riscos (PTR), monitorando o andamento das ações de mitigação;

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

viii. Coordenar com o Encarregado de Proteção de Dados (DPO) as ações relacionadas à conformidade com a LGPD e com os requisitos da ABNT NBR ISO/IEC 27701:2019; e
ix. Apresentar à Alta Direção, em intervalos planejados, relatórios de desempenho do SGSI e do SGPI, incluindo resultados de auditorias internas, indicadores de segurança e status dos objetivos definidos.

4.3 Encarregado de Proteção de Dados – DPO

O Encarregado de Proteção de Dados (DPO), designado em conformidade com o art. 41 da LGPD, atua como ponto focal para questões relacionadas à proteção de dados pessoais, sendo responsável por:

iii. Orientar e fiscalizar o cumprimento da LGPD pelo IPEP e seus colaboradores;
iv. Atender solicitações dos titulares de dados e da ANPD;
v. Elaborar e manter o Registro de Atividades de Tratamento de Dados Pessoais (ROPA);
vi. Recomendar a realização de Relatório de Impacto à Proteção de Dados (RIPD) quando o tratamento representar alto risco; e
vii. Cooperar com o CGSI na implementação dos controles de privacidade previstos na ABNT NBR ISO/IEC 27701:2019.

4.4 Gestores

Os gestores têm a responsabilidade de garantir que sua equipe entenda e siga as orientações desta Política, bem como:

i. Certificar-se que os colaboradores conheçam e respeitem esta Política, além das demais regras de Segurança da Informação;
ii. Orientar sobre o uso adequado das informações e dos recursos tecnológicos;
iii. Comunicar rapidamente ao CGSI qualquer incidente, suspeita de problema ou descumprimento desta Política;
iv. Apoiar ações de conscientização, treinamentos e melhorias relacionadas à Segurança da Informação; e
v. Garantir que os acessos às informações sejam concedidos, revisados e revogados de acordo com a função de cada colaborador.

4.5 Colaboradores

Todos os funcionários, colaboradores, estagiários, aprendizes e demais pessoas que possuam acesso às informações ou recursos do IPEP, são responsáveis pela proteção das informações sob sua guarda, bem como:

i. Cumprir integralmente esta Política e as normas e procedimentos de Segurança da Informação;
ii. Utilizar as informações e os recursos tecnológicos exclusivamente para fins profissionais e autorizados;
iii. Proteger credenciais de acesso, mantendo sigilo sobre senhas e outros mecanismos de autenticação;

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

iv. Comunicar imediatamente ao gestor ou ao CGSI qualquer incidente, suspeita de incidente ou vulnerabilidade identificada; e
v. Evitar práticas que possam comprometer a confidencialidade, integridade ou disponibilidade das informações.

4.6 Fornecedores

São responsabilidades dos Fornecedores:

i. Utilizar as informações exclusivamente para os fins previstos em contrato;
ii. Manter a confidencialidade das informações acessadas;
iii. Adotar medidas de segurança compatíveis com os riscos envolvidos;
iv. Comunicar imediatamente qualquer incidente de Segurança da Informação que possa impactar o IPEP; e
v. Devolver ou eliminar informações ao término do contrato, conforme orientações da organização.

4.7 Clientes e Parceiros

São responsabilidades dos Clientes e Parceiros:

i. Utilizar as informações recebidas de forma ética, segura e conforme o previsto em contrato;
ii. Preservar a confidencialidade das informações compartilhadas;
iii. Comunicar eventuais incidentes de Segurança da Informação relacionados às informações do IPEP; e
iv. Cumprir as obrigações legais, regulatórias e contratuais aplicáveis à Segurança da Informação.

5. USO DE FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL GENERATIVA

5.1 Definição e escopo

Para os fins desta Política, entende-se por Inteligência Artificial Generativa (IAG) qualquer ferramenta, plataforma ou serviço baseado em modelos de linguagem ou outros modelos generativos que produzam conteúdo — textual, de código, de imagem ou de outro tipo — a partir de prompts ou instruções fornecidas pelo usuário, e cujo processamento ocorra total ou parcialmente em infraestrutura de terceiros (nuvem).

Esta seção aplica-se a todas as ferramentas de IAG utilizadas no contexto das atividades do IPEP, incluindo, mas não se limitando a: Figma, Copilot (Microsoft), Claude (Anthropic) e ChatGPT (OpenAI), bem como quaisquer outras ferramentas que venham a ser contratadas ou utilizadas.

5.2 Ferramentas autorizadas e processo de aprovação

O uso de ferramentas de IAG no IPEP é permitido exclusivamente para ferramentas formalmente contratadas pela Alta Direção do IPEP, mediante anuência prévia à contratação,

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

através de parecer técnico que contemple a avaliação de risco feita pelo DPO na redação dos contratos.

O uso de ferramentas de IAG não contratadas pelo IPEP — ainda que gratuitas ou de uso pessoal do colaborador — para atividades relacionadas ao trabalho é expressamente vedado, por configurar risco de vazamento de dados institucionais e de dados pessoais tratados pela organização.

Qualquer nova ferramenta de IAG deve ser submetida ao CGSI para avaliação e aprovação antes de seu uso, mesmo em caráter experimental.

5.3 Classificação de dados e restrições de uso

Tendo em vista que as ferramentas de IAG contratadas processam dados em infraestrutura de terceiros e que, a depender das configurações contratuais, tais dados podem ser utilizados para aprimoramento dos modelos ou retidos por períodos variáveis, é vedado inserir nas ferramentas de IAG, sem exceção, salvo quando a ferramenta estiver operando em modo de processamento contratualmente certificado como não retentivo e não utilizado para treinamento, mediante comprovação documental ao DPO:

- Dados pessoais sensíveis de titulares, conforme definição do art. 5º, ii, da lgpd, incluindo dados previdenciários, dados de saúde, dados econômicos e financeiros individualizados;
- Dados pessoais de clientes, colaboradores, parceiros ou terceiros que permitam identificação direta ou indireta;
- Informações classificadas como confidenciais ou restritas nos termos da política de classificação da informação do ipep, incluindo dados financeiros consolidados, estratégias comerciais e informações de auditorias internas;
- Credenciais de acesso, tokens, chaves de api, senhas ou quaisquer segredos de autenticação;
- Integração ilimitada com a nuvem de arquivos (onedrive); e
- Dados protegidos por sigilo legal ou regulatório aplicável à atividade do IPEP.

5.4 Responsabilidades dos usuários

Todo colaborador que utilize ferramentas de IAG no exercício de suas funções é individualmente responsável por:

- Verificar, antes de elaborar qualquer prompt, se as informações que pretende inserir se enquadram nas restrições do item 5.3;
- Não compartilhar outputs gerados por iag que contenham dados sensíveis ou confidenciais sem prévia revisão e aprovação de seu gestor;
- Reportar imediatamente ao cgsi ou ao dpo qualquer situação em que dados protegidos tenham sido inadvertidamente inseridos em uma ferramenta de iag; e

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

- Não utilizar os outputs de ferramentas de IAG como fonte única de decisões que afetem direitos ou obrigações de titulares de dados pessoais, bem como de conclusão do conteúdo gerado, EXIGINDO SEMPRE REVISÃO HUMANA QUALIFICADA.

5.5 Obrigações específicas relativas à privacidade e à LGPD

As ferramentas de IAG contratadas pelo IPEP são tratadas como operadores de dados pessoais para fins da LGPD e da ISO 27701:2019, sempre que houver possibilidade de processamento de dados pessoais por meio de seu uso. Nessa condição, o IPEP deve assegurar que os contratos de prestação de serviço com os fornecedores de IAG contenham cláusulas adequadas de proteção de dados, em conformidade com o art. 39 da LGPD e com o controle A7.2.6 da ISO 27701:2019, e que tais contratos sejam revisados pelo DPO antes de cada renovação.

O DPO é responsável por avaliar a necessidade de elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para os fluxos de trabalho que envolvam uso de IAG com dados pessoais, conforme o art. 38 da LGPD.

5.6 Monitoramento e auditoria

O CGSI poderá, a qualquer tempo e com comunicação prévia, auditar o uso das ferramentas de IAG no ambiente de trabalho do IPEP, incluindo a revisão de logs de acesso disponibilizados pelos fornecedores e a análise de eventuais incidentes relatados.

O uso das ferramentas de IAG em desconformidade com esta Política será tratado como incidente de segurança da informação, sujeito às medidas disciplinares previstas no item 7 e demais instrumentos normativos internos do IPEP.

5.7 Revisão e atualização

Dado o ritmo acelerado de evolução das tecnologias de IAG e da regulação aplicável, esta seção deverá ser revisada pelo CGSI em prazo não superior a doze meses a partir de sua publicação, ou antes, caso ocorra:

i. Contratação ou descontinuação de ferramenta de IAG;
ii. Atualização relevante dos termos de serviço dos fornecedores contratados;
iii. Publicação de regulamentação específica sobre IA pela ANPD, pelo Congresso Nacional ou por órgão regulador setorial competente; ou
iv. Identificação de incidente de segurança relacionado ao uso de IAG.

6. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

O IPEP adota abordagem formal e estruturada para a avaliação e o tratamento de riscos de segurança da informação e privacidade, em conformidade com os requisitos das cláusulas 6.1 e 6.2 da ABNT NBR ISO/IEC 27001:2022 e com a cláusula 6.3 da ABNT NBR ISO/IEC 27701:2019.

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

O processo de gestão de riscos compreende as seguintes etapas:

i. Identificação dos ativos de informação e dos riscos a que estão sujeitos;
ii. Análise e avaliação dos riscos com base em critérios de probabilidade e impacto definidos pelo CGSI;
iii. Definição das opções de tratamento de risco (mitigar, aceitar, transferir ou evitar);
iv. Implementação do Plano de Tratamento de Riscos (PTR), com responsáveis e prazos definidos; e
v. Monitoramento contínuo e revisão periódica dos riscos e controles implementados.

Os riscos de privacidade, incluindo aqueles relacionados ao tratamento de dados pessoais, são avaliados e tratados em conjunto com o DPO, considerando os direitos e interesses dos titulares de dados e as obrigações da LGPD.

7. SANÇÕES E MEDIDAS DISCIPLINARES

O descumprimento, ainda que por omissão, negligência ou tentativa não consumada, das disposições desta Política, bem como de quaisquer outras normas, procedimentos ou controles de segurança da informação e privacidade, poderá resultar na aplicação de medidas disciplinares e sanções, observados os princípios da proporcionalidade, razoabilidade e devido processo.

Para os colaboradores regidos pela Consolidação das Leis do Trabalho (CLT), as sanções poderão incluir, conforme a gravidade da infração e a legislação aplicável, advertência verbal, advertência formal por escrito, suspensão sem remuneração e, nos casos mais graves, a rescisão do contrato de trabalho por justa causa.

No caso de colaboradores pessoas jurídicas, prestadores de serviço, parceiros comerciais ou cooperados, o descumprimento poderá ensejar a aplicação de penalidades contratuais, incluindo, quando aplicável, a rescisão imediata do contrato, sem prejuízo de outras medidas legais cabíveis.

A definição e aplicação das sanções serão fundamentadas em avaliação conduzida pelo Comitê Gestor de Segurança da Informação (CGSI), considerando, entre outros fatores, a natureza e a gravidade da infração, o impacto à segurança da informação, à privacidade e à proteção de dados pessoais, o grau de responsabilidade, bem como a reincidência.

Sempre que caracterizada infração relevante, o CGSI poderá comunicar formalmente o fato ao gestor imediato do envolvido, que será responsável pela aplicação da penalidade cabível, após a devida apuração e confirmação da falta, garantindo-se o registro das decisões e a rastreabilidade do processo.

8. AUDITORIA INTERNA, MONITORAMENTO E MELHORIA CONTÍNUA

O IPEP realiza auditorias internas em intervalos planejados para verificar se o SGSI e o SGPI estão em conformidade com os requisitos das normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019, e se estão implementados e mantidos de forma eficaz.

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br

O CGSI, com o apoio do DPO, monitora, mede, analisa e avalia o desempenho do SGSI e do SGPI por meio de indicadores de segurança e privacidade definidos em documento específico, reportando os resultados à Alta Direção na análise crítica periódica prevista na cláusula 9.3 da ABNT NBR ISO/IEC 27001:2022.

Não conformidades identificadas, seja em auditorias internas ou externas, em incidentes ou em revisões periódicas, ensejarão a implementação de ações corretivas documentadas, com análise de causa raiz, definição de responsável e prazo de tratamento, conforme cláusula 10.1 da ABNT NBR ISO/IEC 27001:2022.

Esta Política deve ser revisada pelo menos anualmente ou sempre que ocorrerem mudanças significativas no contexto organizacional, nos riscos identificados, na legislação aplicável ou nos requisitos das normas de referência, cabendo ao CGSI propor as atualizações necessárias para aprovação da Alta Direção.

9. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As orientações apresentadas nesta política e nas outras normas e processos de segurança não se limitam devido à evolução tecnológica incessante e à emergência contínua de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação do IPEP adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações e dados pessoais.

10. HISTÓRICO DAS ALTERAÇÕES

Data	Revisão	Histórico
19/12/2025	01	Aprovação inicial
03/05/2026	02	Revisão para adequação aos requisitos das normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019 e à LGPD

(19) 9.9915-3727 institucional@ipepbrasil.org.br www.institutoipep.org.br