INSTITUTO DE BIOLOGIA MOLECULAR DO PARANÁ - IBMP

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE (PSIP)

Fornecedores, Prestadores de serviços e Terceiros

CLASSIFICAÇÃO: pública

1. OBJETIVO

A Política de Segurança da Informação e Privacidade (PSIP) para Fornecedores, Prestadores de Serviços e Terceiros, doravante apenas "TERCEIROS", tem como objetivo apresentar os requisitos mínimos de segurança que devem ser observados por essas partes, com a finalidade de garantir a proteção dos ativos do ***IBMP***.

Por isso, cabe a cada ***TERCEIRO*** que mantenha relação com o ***IBMP*** estabelecer, implementar e manter um sistema de gestão de segurança da informação para preservar a confidencialidade, integridade e disponibilidade das informações e dados pessoais aos quais venha a ter acesso em decorrência de seu relacionamento com o ***IBMP***.

As diretrizes previstas nesta PSIP devem ser observadas para garantir a proteção das informações e dados pessoais disponibilizadas pelo ***IBMP***, bem como estabelecer o uso adequado de seus sistemas de informação acessados pelos ***TERCEIROS*** em razão do relacionamento mantido com o ***IBMP***.

2. ABRANGÊNCIA

Todos os ***TERCEIROS*** vinculados ao ***IBMP***.

3. CICLO DE VIDA DA PSIP

A PSIP foi desenvolvida pelas áreas de TI, GRC e JURÍDICO do IBMP, com o apoio da Datalege (DPO), e sua vigência inicia a partir da data de sua aprovação e publicação no site do ***IBMP***, revogando e substituindo as versões anteriores. Esta PSIP será revista anualmente ou atualizada ou a qualquer tempo, a exclusivo critério do ***IBMP***, sempre que algum fato relevante ou evento motive sua revisão antecipada.

4. DIRETRIZES GERAIS

4.1 Princípios

As Partes indicadas no item 2 devem observar, de imediato, os princípios previstos no art. 6º da Lei Geral de Proteção de Dados Pessoais, sem prejuízo de garantir:

- A proteção da informação e/ou de dados pessoais todos os níveis da cadeia de fornecimento e/ou prestação de serviço.
- A confidencialidade, autenticidade, integridade e disponibilidade das informações a que tenham acesso.
- O cumprimento das exigências definidas pelo ***IBMP*** para assegurar a proteção de suas informações e/ou dados pessoais.

5. DEFINIÇÕES

5.1 Para fins do disposto nesta PSIP, considera-se:

(a) **Documento**: unidade de registro de informações, independentemente do formato, do suporte ou da natureza.

(b) **Fornecedores, Prestadores de serviço e Terceiros**: doravante apenas "TERCEIRO", entidades ou pessoas externas ao ***IBMP*** que tenham acesso aos sistemas de informação e/ou dados pessoais do Instituto.

(c) **Incidente de Segurança da Informação:** evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de qualquer ativo, independentemente de sua natureza, do ***IBMP***.

(d) **Informação:** todo dado, independentemente do meio, suporte ou formato, que tenha sido processado, organizado, estruturado, correlacionado ou contextualizado de modo a adquirir significado, utilidade ou valor para quem o utiliza. Incluem-se na definição de Informação, para todos os fins, os conceitos de dado pessoal e de dado pessoal sensível, conforme definidos na Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

(e) **Operação:** o mesmo que "Tratamento".

(f) **Sistema de informação:** trata-se, de maneira exemplificativa e não exaustiva, do conjunto de aplicações, serviços, ativos de tecnologia da informação ou outros componentes de manuseio de **informações**. Os ativos dividem-se em (i) *ativos primários* como, mas sem se limitar, a

informação, processos de negócios e atividades; e (ii) *ativos de suporte* como, não se limitando, *hardware*, *software*, redes, pessoal, local, estrutura da do ***IBMP***.

(g) **Tratamento:** toda operação realizada com as **informações** do ***IBMP***, incluindo, mas não se limitando, as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

6. CONTROLES

A presente Política de Segurança da Informação e Privacidade define controles de referência a serem observados pelos terceiros, cuja implementação deverá ocorrer de forma proporcional e baseada em risco, devendo tais controles ser adaptados à realidade operacional de cada terceiro.
Para assegurar a proteção dos ativos do IBMP tratados em decorrência da relação entre as partes, o TERCEIRO deverá implementar, no mínimo, os controles e diretrizes estabelecidos a seguir.

6.1. CONTROLES ORGANIZACIONAIS

6.1.1. Política de Segurança da Informação e Privacidade

Implementar, com o apoio da Alta Direção, uma Política de Segurança da Informação e Privacidade (PSIP) para assegurar a adequação contínua, suficiência, efetividade da direção de gestão e suporte à segurança dos ativos do ***IBMP***. Caberá ao ***TERCEIRO*** garantir a proteção das **informações** do ***IBMP*** em todo seu ciclo de vida.

6.1.2. Papéis e responsabilidade pela segurança da informação

Definir responsabilidades e estabelecer uma estrutura de gestão de segurança, responsável por implementar e analisar criticamente a PSIP periodicamente.

6.1.3. Segregação de funções

Separar funções conflitantes entre diferentes indivíduos para evitar execuções não supervisionadas de tarefas críticas. Cabe ao ***TERCEIRO*** determinar quais funções e áreas de responsabilidade precisam ser segregadas.

6.1.4. Gestão de ativos

Desenvolver e manter um inventário dos, mas não se limitando a, sistemas de informação que serão utilizados nas atividades de tratamento das informações do ***IBMP***. Cabe ao ***TERCEIRO*** mapear o fluxo das informações e/ou dados pessoais, isto é, como são coletados, por quem, finalidade do tratamento, local de armazenamento, com quem são compartilhados, quais os meios técnicos e administrativos de segurança adotados, entre outros. Os gestores, como proprietário do mapeamento de sua área, têm a responsabilidade de mantê-lo sempre atualizado.

6.1.5. Inteligência de ameaças

Coletar e analisar informações sobre ameaças para aplicar ações de prevenção e mitigação adequadas.

6.1.6. Segurança da informação no gerenciamento de projetos

Integrar a segurança em todas as fases de projetos para tratar riscos desde os estágios iniciais.

6.1.7. Uso aceitável de informações e dados pessoais

Implementar regras de manuseio e garantir que colaboradores e agentes externos estejam conscientes dos requisitos de segurança para as informações do ***IBMP.*** O ***TERCEIRO*** deve garantir que seus colaboradores e agentes externos que usem ou tenham acesso aos Ativos do ***IBMP*** estejam conscientes dos requisitos de segurança da informação.

6.1.8. Uso de plataformas de videoconferência

Durante a relação existente entre o *IBMP* e o *TERCEIRO*, todas as reuniões realizadas por meio de plataformas de videoconferência, independentemente de serem promovidas pelo *IBMP* ou pelo *TERCEIRO*, deverão observar integralmente as disposições desta cláusula:

- **Plataformas:** Utilizar exclusivamente Teams, Zoom ou Google Meet (contas corporativas).
- **Acesso:** Aplicar senhas, salas de espera e MFA/SSO sempre que disponível.
- **Segurança:** Proibido o uso de ferramentas de IA para transcrição ou gravação sem autorização prévia do IBMP.
- **Incidentes:** Notificar o IBMP sobre qualquer falha ou acesso não autorizado em até 24 horas.

- **Conduta:** Utilizar nome e identificação corretos, manter a postura profissional e linguagem adequada.
- Compartilhamento de Tela: Compartilhar somente a janela ou documento necessário para a pauta da reunião.

6.1.9. Devolução de Ativos

Devolver ou eliminar (de forma irrecuperável) informações e ativos físicos do IBMP em até 30 dias após o término da relação contratual, mediante declaração formal de exclusão.

6.1.10. Classificação das informações

Tratar todas as informações do IBMP como confidenciais e restringir o acesso apenas a quem possua efetiva necessidade de conhecimento. Todos os colaboradores do ***TERCEIRO*** devem ser comunicados, por escrito, sobre a obrigação de tratarem todas as **informações** como confidenciais e cumprirem os requisitos legais relativos à confidencialidade, autenticidade, integridade e disponibilidade.

6.1.11. Transferência de informações

Implementar proteção contra interceptação e garantir a rastreabilidade/não repúdio das informações em trânsito.

6.1.12. Controle de acessos

Estabelecer privilégios estritos, utilizar autenticação forte (duplo fator) e revogar acessos imediatamente em casos de mudança de função ou desligamento. O TERCEIRO deve se comprometer a respeitar as áreas restritas e somente acessar de acordo a instrução recebida no momento da sua integração.

6.1.13. Abordagem em contratos com suboperadores

Documentar e garantir que eventuais suboperadores cumpram integralmente os requisitos de segurança e proteção de dados do IBMP.

6.1.14. Gestão de segurança na cadeia de fornecimento de TIC

Aplicar medidas de mitigação de riscos em toda a cadeia de fornecedores de tecnologia

relacionados ao serviço.

6.1.15. Gestão de incidentes de segurança da informação

Estabelecer processos de resposta rápida e ordenada, operados por equipe designada, para gerenciar eventos de segurança.

6.1.16. Coleta de evidências

Implementar procedimentos para preservar a autenticidade e integridade de registros relacionados a eventos de segurança.

6.2. CONTROLE DE PESSOAS

6.2.1. Acordos de confidencialidade

Firmar com os colaboradores que irão tratar as informações do ***IBMP*** um acordo de confidencialidade.

6.2.2. Relato de eventos de segurança

Comunicar incidentes de segurança envolvendo as informações do IBMP em até 24h para o DPO pelo canal dpo@ibmp.org.br.

6.3. CONTROLES FÍSICOS

6.3.1. Perímetros e Entradas Físicas

Aplicar barreiras e controles de acesso para proteger áreas que contenham informações e sistemas do IBMP.

6.3.4. Mesa limpa e tela limpa

Bloquear dispositivos automaticamente quando sem supervisão e garantir o armazenamento seguro de documentos e mídias físicas.

6.3.6. Descarte seguro de equipamento

Remover informações do IBMP de maneira irrecuperável antes do descarte ou reutilização de hardwares.

6.4. CONTROLES TECNOLÓGICOS

6.4.1. Dispositivos endpoint

Garantir antivírus, firewall, criptografia de disco e proibição de armazenamento local (fora da rede/ambiente autorizado) nos dispositivos dos colaboradores.

6.4.3. Proteção contra malware

O ***TERCEIRO*** que mantenha relação contratual com o ***IBMP*** deverá implementar e manter soluções tecnológicas adequadas para a detecção, prevenção e mitigação de ameaças decorrentes de códigos maliciosos, bem como adotar medidas de conscientização de seus colaboradores quanto aos riscos relacionados à segurança da informação.

Todo, sem se limitar, arquivo, documento, conteúdo digital, a ser enviado ao ***IBMP***, deverá ser previamente verificado pelo ***TERCEIRO***, por meio de solução de segurança apropriada, com a finalidade de identificar a existência de códigos maliciosos.

O envio de qualquer arquivo, documento ou conteúdo digital ao ***IBMP*** fica condicionado à prévia confirmação, pelo ***TERCEIRO***, da inexistência de códigos maliciosos nos materiais encaminhados, constituindo o cumprimento deste controle requisito obrigatório para a prestação dos serviços contratados.

6.4.5. Backup e Logs

Manter backups seguros (fora do local principal) com testes de restauração e registrar logs de atividades para auditoria e investigação.

7. SANÇÕES E PENALIDADES

O ***IBMP*** realiza o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política. Caso o ***TERCEIRO*** viole qualquer uma das regras aqui dispostas, bem como a LGPD e demais legislações aplicáveis, mesmo que por omissão ou tentativa não consumada, será considerado como um incidente de Segurança da Informação e poderá acarretar a rescisão de eventual contrato firmado entre as partes e a aplicação das medidas judiciais e administrativas cabíveis.

O ***TERCEIRO*** se declara ciente de que é o único responsável pelos incidentes de segurança a que comprovadamente der causa e deverá reparar integralmente os prejuízos suportados pelo ***IBMP***.
Em sendo o ***IBMP*** responsabilizado administrativamente e/ou judicialmente em razão da ação ou omissão, culpa ou dolo, exclusiva e comprovada do ***TERCEIRO*** em decorrência da violação e/ou descumprimento desta PSIP, fica garantido ao ***IBMP*** o direito de denunciação da lide, nos termos do artigo 125, II, do Código de Processo Civil, com o objetivo de exigir do ***TERCEIRO*** o ressarcimento de todos os danos e prejuízos de qualquer natureza que suportou incluindo, mas não se limitando, indenizações, multas, honorários advocatícios, custas processuais.

8. DISPOSIÇÕES FINAIS

O ***TERCEIRO*** poderá enviar suas dúvidas sobre esta PSIP ou sugestões visando seu aprimoramento para o Coordenador de Segurança da Informação pelo canal indicado no item 6.2.2.
O ***TERCEIRO*** deverá ler e cumprir integralmente as diretrizes estabelecidas nesta "Política de Segurança da Informação e Privacidade para ***TERCEIROS*** do ***IBMP***.

APROVAÇÃO

Esta Política de Segurança da Informação e Privacidade (PSIP) foi aprovada pela Alta Direção em 13/04/2026.

HISTÓRICO DE VERSÕES

Versão	Data	Descrição das Alterações	Elaboração / Revisão	Aprovação
1.1	30/10/2026	Retirada do CSP	STI	Alta Direção

ATUALIZAÇÃO E VIGÊNCIA

Após a aprovação pela Alta Direção, esta Política de Segurança da Informação e Privacidade para ***TERCEIROS*** (PSIP - ***TERCEIROS***) entra em vigor na data de sua publicação e passa a ser de observância obrigatória por todos aqueles que a ela se submetem.
A PSIP poderá ser atualizada sempre que necessário, em decorrência de alterações legais ou regulatórias

aplicáveis, bem como em razão da ocorrência de incidentes de segurança ou de privacidade que demandem ajustes ou aprimoramentos. Eventuais atualizações serão formalizadas e devidamente comunicadas a todos os destinatários desta PSIP - ***TERCEIROS***, produzindo efeitos a partir de sua divulgação.