1. Objetivos

A Política de Segurança da Informação do Instituto tem como objetivo garantir a confidencialidade, integridade e disponibilidade das informações, bem como a proteção dos ativos de informação contra ameaças internas e externas. Esta política estabelece os princípios e responsabilidades gerais de segurança da informação para todos os funcionários, contratados e partes interessadas da empresa.

Os principais objetivos da Política de Segurança da Informação são:

- Proteger as informações da empresa contra acesso, divulgação, modificação, destruição ou interrupção não autorizados.
- Cumprir as leis e regulamentações de proteção de dados aplicáveis.
- Garantir a continuidade dos negócios, minimizando o impacto de incidentes de segurança da informação.
- Gerenciar os riscos de segurança da informação de forma proativa e eficaz.

2. Abrangência

Classificação da Informação (Conforme GES-004)	( ) Pública (X) Interna ( ) Restrita ( )Confidencial ( ) Secreta
Conhecimento de Publicação	Desenvolvimento de Negócios, Desenvolvimento Tecnológico, Jurídico e GRC, Assessoria de Comunicação, Gestão Estratégica, Operações Corporativas, Produção e Qualidade.
Posto de Cópias	PSI terceiros - Documento 009.000042 (site do IBMP)

3. Definições

Ativo: Qualquer recurso que tenha valor para a Organização.

BPx: Boas Práticas onde x pode ser fabricação, distribuição, laboratório, etc. Podemos dizer que todos e quaisquer softwares e hardwares que tenham impacto na saúde do paciente, qualidade do produto e integridade de dados.

Confidencialidade: Garantia de que a informação é acessível somente por pessoas autorizadas.

Controle: Mecanismo de gerenciamento de risco, incluindo políticas, procedimentos, diretrizes e estruturas organizacionais.

DPO: O DPO (*Data Protection Officer*, ou Encarregado pelo Tratamento de Dados Pessoais) é o profissional responsável por garantir que uma organização esteja em conformidade com as leis de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasi

Endpoints: Dispositivos de armazenamento e processamento de informação, como computadores, celulares e tablets utilizados na Organização.

Hotspot Móvel: Função que permite compartilhar a conexão de internet de um smartphone, tablet ou modem portátil com outros dispositivos, como laptops e tablets. Ele utiliza a rede celular para criar uma conexão Wi-Fi, permitindo acesso à internet em qualquer lugar com cobertura de rede móvel.

Incidente de Segurança da Informação: Evento indesejado ou inesperado que compromete as operações de negócios e ameaça à segurança da informação.

Log: Registro de atividades realizadas em sistemas.

Meio Eletrônico: Forma de armazenamento ou tráfego de documentos digitais.

Nuvem Pública: Serviços de computação oferecidos por terceiros via internet.

Nuvem Privada: Serviços de computação em nuvem restritos a usuários autorizados.

Transmissão eletrônica: Transferência de dados digitais por canais de comunicação.

VPN (Virtual Private Network): Rede privada que permite acesso remoto seguro a uma rede corporativa.

Vulnerabilidade: Fragilidade que pode ser explorada por ameaças.

4. Responsabilidades

Todos os Colaboradores:

- Conhecer e aderir às políticas, procedimentos e diretrizes de segurança da informação da Instituição.
- Reportar incidentes de segurança da informação imediatamente aos canais apropriados.
- Proteger os ativos de informação da Instituição contra acessos não autorizados.
- Utilizar os recursos de informação da Instituição de forma responsável e ética.

Equipe de Segurança da Informação:

- Implementar e manter os controles de segurança da informação definidos nesta política e em outras políticas relacionadas.
- Realizar avaliações regulares de riscos e vulnerabilidades dos ativos de informação da empresa.
- Desenvolver e manter planos de resposta a incidentes de segurança da informação.
- Monitorar continuamente os sistemas, redes e atividades relacionadas à segurança da informação em busca de possíveis ameaças e violações.
- Investigar e responder prontamente à incidentes de segurança da informação, adotando medidas corretivas apropriadas.
- Fornecer treinamento e conscientização em segurança da informação para funcionários e contratados (Periodicidade Anual).
- Garantir a conformidade com as políticas e padrões de segurança da informação, bem como com as leis e regulamentos aplicáveis.

- Realizar revisões e auditorias periódicas para avaliar a eficácia dos controles de segurança da informação.
- Manter-se atualizado sobre as tendências e as melhores práticas em segurança da informação e propor melhorias contínuas.
- Colaborar com outras equipes e partes interessadas relevantes para garantir a segurança da informação em toda a empresa.
- Monitorar e revisar regularmente o cumprimento desta política e relatar as descobertas e recomendações à Executiva.

5. Diretrizes Gerais

A política de segurança da informação é um conjunto de diretrizes e regras que define como uma organização protege seus dados e sistemas contra ameaças internas e externas. Ela estabelece responsabilidades, controles e procedimentos para garantir confidencialidade, integridade e disponibilidade das informações. As medidas para a proteção de informações críticas da empresa devem levar em consideração o impacto (valor) para o negócio associado com o acesso não autorizado ou perda de informações BPx críticas. A Política de Segurança da Informação deve ser documentada, revisada periodicamente, pela equipe de TI e comunicada a todos os funcionários, contratados e partes interessadas relevantes. O acesso à política deve ser controlado, e a documentação associada deve ser mantida atualizada.

5.1 Classificação das Informações e Armazenamento de dados Críticos

O GES-004 estabelece diretrizes para proteger e organizar as informações da organização, garantindo segurança contra vazamento e acesso não autorizado. Deve ser divulgado internamente de forma clara e adaptada às funções e à sensibilidade das informações, com um resumo acessível ao público externo, aplicando-se a todos os membros internos e externos (prestadores de serviços e parceiros) que acessam as informações da organização. Para a classificação das informações, devem ser considerados aspectos relacionados à confidencialidade, integridade, disponibilidade e valor da informação, sendo estas classificadas como públicas, internas, restritas, confidenciais ou secretas, conforme descrito no GES-004. Documentos em papel contendo informações críticas devem ser arquivados ou recolhidos quando não estiverem em uso. Após utilizar impressoras ou equipamentos de fax, todos os documentos em papel devem ser removidos, e, caso o equipamento armazene cópias eletrônicas de documentos sensíveis, estas devem ser excluídas. Além disso, mídias em papel ou filme contendo informações críticas devem ser destruídas utilizando processos aprovados, como trituração, antes do descarte.

No mínimo, as informações críticas para o Instituto de Biologia Molecular do Paraná (IBMP) ou de seus clientes armazenadas em computadores devem estar protegidas por senha tanto no nível do computador

do usuário quanto no nível de acesso à rede. É incentivado o uso de proteção criptográfica aprovada para informações críticas. Informações críticas armazenadas em dispositivos de armazenamento removível, como HDs portáteis ou tokens/pen drives USB, devem ser criptografadas utilizando criptografia aprovada ou controladas fisicamente, garantindo proteção contra perda, roubo e acesso não autorizado. As informações críticas do IBMP e de seus clientes incluídas em backups realizados pelos administradores em mídias removíveis devem ser armazenadas em locais seguros e manter uma cópia fora da empresa.

5.2 Backup

Este capítulo define as diretrizes e responsabilidades para o processo de backup e restauração de dados da organização, visando assegurar a integridade, disponibilidade e confiabilidade dos dados críticos. Aplica-se à equipe de Infraestrutura e Segurança da Informação e a todos os ambientes onde dados institucionais estejam armazenados (on-premises e nuvem).

Proteção e Armazenamento: Os backups devem ser armazenados em locais seguros, com mecanismos de imutabilidade e redundância (incluindo repositórios externos/nuvem), protegendo contra perdas e incidentes.

Controle de Acesso: O acesso aos consoles e ferramentas de backup é restrito a pessoas autorizadas, exigindo autenticação forte (MFA) e privilégio mínimo conforme os padrões de controle de acesso.

Limites de Escopo: O serviço de backup corporativo contempla exclusivamente os servidores, sistemas e repositórios oficiais centralizados. Arquivos armazenados localmente em estações de trabalho (*endpoints*), dispositivos móveis ou mídias removíveis **não** são objeto de cópia ou recuperação.

O escopo detalhado de ativos contemplados, frequências de cópia, prazos de retenção, procedimentos de restauração e rotinas de testes periódicos estão formalizados no POP ADM-007.

5.3 Gestão de Senhas

A gestão de senhas é um dos pilares da segurança da informação e tem como objetivo garantir que o acesso aos sistemas, aplicações e informações sensíveis da organização seja restrito a usuários autorizados. Este controle é essencial para reduzir o risco de acessos não autorizados, vazamento de informações e outros incidentes de segurança.

A criação de senhas deve seguir diretrizes rigorosas para assegurar que elas sejam fortes e difíceis de serem comprometidas.

As senhas utilizadas pelos usuários nos sistemas internos do IBMP devem obedecer aos seguintes requisitos mínimos:

- As senhas devem ter no mínimo 8 caracteres.
- As senhas devem conter três dos quatro requisitos de complexidade (letras maiúsculas, letras minúsculas, números e caracteres especiais).

- Evitar senhas que incluam informações pessoais como nome, data de nascimento ou número de telefone, de modo a dificultar tentativas de adivinhação.
- Palavras comuns, como “senha” ou “123456”, são proibidas, assim como sequências de teclado (ex.: "qwerty").
- A senha deve ser alterada a cada 45 dias, ou em intervalos menores, dependendo da criticidade do sistema acessado.
- A senha não poderá ser igual às últimas 10 senhas utilizadas
- A senha não pode conter o nome da conta do usuário ou partes do nome completo do usuário que excedam dois caracteres consecutivos.

A autenticação multifatorial (MFA) é altamente recomendada para sistemas críticos conforme análise documentada no Inventário de Sistemas Computadorizados (FPOP-VAR-005-01) e apoio da área de segurança da informação do IBMP.

Para que a segurança das senhas seja efetiva, todos os colaboradores devem seguir as melhores práticas de uso e manutenção, como:

- É estritamente proibido compartilhar senhas entre usuários ou com terceiros, exceto em casos excepcionais devidamente autorizados e auditados.
- As senhas corporativas não devem ser reutilizadas em outras contas, especialmente em contas de uso pessoal.
- Em caso de suspeita de comprometimento da senha, o usuário deve alterá-la imediatamente e notificar a área de segurança da informação através do e-mail ti@ibmp.org.br ou abertura de chamado conforme POP ADM-015.
- Os usuários devem estar atentos a tentativas de phishing que busquem capturar suas credenciais, evitando clicar em links suspeitos ou compartilhar senhas por e-mail.

Todos os usuários da organização são responsáveis pelo cumprimento das políticas de gestão de senhas estabelecidas nesta política.

5.4 Segurança de Redes

Aplica-se a todos os *endpoints* e conexões que compõem a infraestrutura de rede do IBMP.

O IBMP monitora todo tráfego de rede continuamente para detectar atividades suspeitas ou anômalas, utilizando ferramentas apropriadas de análise de tráfego.

Práticas Proibidas:

- É estritamente proibido o uso de redes privadas virtuais (VPNs) externas, públicas ou gratuitas, para acessar sistemas da organização. Apenas VPNs autorizadas pela equipe de segurança da informação devem ser utilizadas, pois serviços externos podem expor dados sensíveis e comprometer a segurança da rede.

- *Endpoints* pessoais não devem ser conectados à rede corporativa sem autorização da equipe de TI. Dispositivos pessoais podem não ter os níveis de segurança exigidos e podem introduzir vulnerabilidades na rede.
- Cada colaborador deve manter suas credenciais seguras e privadas. O compartilhamento de senhas ou a utilização de credenciais de outros é estritamente proibido, pois compromete a segurança de acesso e dificulta a identificação de atividades não autorizadas.
- Todos os softwares instalados nos dispositivos corporativos devem ser autorizados previamente pela equipe de segurança de TI. Softwares não autorizados podem conter vulnerabilidades ou funcionalidades que afetam a segurança dos sistemas. Mais informações sobre softwares vide POP ADM-102.
- O armazenamento ou transferência de dados corporativos em dispositivos pessoais ou serviços de armazenamento em nuvem sem autorização da TI é proibido. Essas práticas colocam dados em risco de exposição e violam a política de segurança.

5.5 Gestão de Ativos

A gestão de ativos de tecnologia da informação visa assegurar o controle, a proteção e a adequada utilização dos equipamentos e dispositivos fornecidos aos colaboradores para o exercício de suas funções. Estes ativos incluem computadores, celulares, tablets, redes, softwares e quaisquer outros dispositivos ou sistemas disponibilizados pela empresa.

Os colaboradores são responsáveis por utilizar os ativos de TI exclusivamente para finalidades profissionais. O uso inadequado, como reparos não autorizados ou instalação de software não licenciado, é proibido. Em caso de danos ou problemas, os colaboradores devem abrir um chamado de suporte, conforme as instruções do POP ADM-015.

Regras Gerais:

- Equipamentos podem ser solicitados no momento da contratação ou posteriormente, mediante a necessidade aprovada pelo setor de Recursos Humanos e pela equipe de TI.
- Ao desligar-se do IBMP ou sempre que solicitado, o colaborador deve devolver todos os dispositivos e acessórios em boas condições de uso, desconsiderando o desgaste natural. Qualquer dano deverá ser reportado à TI.
- Os ativos cedidos são de uso exclusivo do colaborador e devem ser preservados. Alterações de hardware, troca, venda ou cessão de dispositivos são terminantemente proibidos. Equipamentos danificados por mau uso ou modificações não autorizadas podem gerar responsabilização para o colaborador.

- Em caso de roubo ou extravio, o colaborador deve informar imediatamente e apresentar um boletim de ocorrência, para que a empresa tome as medidas de bloqueio e rastreamento, conforme necessário.

  O IBMP pode, a qualquer momento, realizar auditorias nos equipamentos para garantir o uso conforme a política de segurança e o compliance. Dados produzidos e armazenados nos dispositivos fornecidos são considerados propriedade exclusiva da empresa, e os colaboradores devem garantir que tais informações sejam usadas e tratadas conforme as políticas de proteção de dados pessoais (GES-020).

5.6 Segurança Física e do Ambiente

A segurança física e a proteção do perímetro são fundamentais para garantir a integridade dos ativos, a proteção das áreas sensíveis e a continuidade das operações institucionais.

Mecanismos de Controladoria: As instalações devem possuir controles formais de acesso (ex.: crachás, biometria ou credenciais equivalentes), garantindo que apenas pessoas autorizadas ingressem em setores restritos.

Identificação Pessoal: É obrigatório o uso visível de crachá de identificação por todos os colaboradores e terceiros nas dependências do instituto. Em caso de perda, roubo ou extravio, a ocorrência deve ser notificada imediatamente aos responsáveis para bloqueio das credenciais.

Acesso de Terceiros e Visitantes: A entrada e a permanência de prestadores de serviços, terceiros e visitantes são condicionadas à prévia autorização, identificação e alinhamento com as normas de segurança vigentes. A política de segurança para terceiros (documento 009.000042) está publicada no site do IBMP disponível para consulta.

Concessão e Revogação de Acessos: Os perfis de acesso físico são atribuídos com base na necessidade da função (*menor privilégio*) e mediante aprovação formal. Os acessos devem ser revogados imediatamente em casos de desligamento, afastamento ou término de contrato.

As rotinas detalhadas de cadastro, concessão de permissões, treinamento de terceiros, monitoramento de visitantes e fluxos de desligamento estão estabelecidas no **POP ADM-047**.

5.7 Controle de Acesso Lógico

O sistema de controle de acesso do IBMP é estruturado com base em autenticação rigorosa, uso de autenticação multifator (MFA) e segregação de privilégios quando implementados pela área de TI. Esses controles são aplicados a recursos como redes internas, servidores, aplicações e bancos de dados. Além disso, práticas de auditoria, como a manutenção de registros de acesso e revisões periódicas, são executadas para garantir que os usuários mantenham apenas os acessos necessários às suas funções.

Desta forma, o controle de acesso não só protege os ativos da organização, mas também promove a responsabilidade individual e a segurança operacional, reforçando a confiança nos sistemas de informação utilizados.

- Não é permitido acessar sistemas ou informações sem a devida autorização;
- É proibido o uso de credenciais genéricas para múltiplos usuários, ou seja, cada colaborador deve ter suas próprias credenciais exclusivas;
- Compartilhamento de senhas é estritamente proibido, independentemente do nível hierárquico;
- Não é recomendado o acesso remoto de estações públicas como cybercafés, quiosques de internet ou terminais públicos, é proibido o uso em redes abertas que não possuam método de autenticação, sendo recomendado o uso de hotspot móvel, conforme descrito no procedimento GES-001.
- É estritamente proibido alterar a data e hora dos servidores, mesmo para usuários com acesso administrativo;
- Não é permitido utilizar contas de serviço para realizar login interativo nos sistemas.
- O uso de equipamentos não autorizados para acessar a rede interna é proibido.
- Modems ou equipamentos similares não são pontos de entrada autorizados para acesso remoto
- O uso de redes públicas não criptografadas para transmitir informações é proibido.
- Os desktops (estações de trabalho) possuem acesso com senha, e possuem opção de bloqueio de tela e time-out.
- O time-out do Windows deve ser programado para ocorrer após 5 minutos de inatividade por parte do usuário.

5.8 Segurança dos Equipamentos

Apenas pessoal de manutenção autorizado pode executar manutenção e reparos em equipamentos, sendo mantido registro de falhas e das ações realizadas. Equipamentos que dependem de energia elétrica devem ser protegidos contra falta de energia, picos e outras variações, com uso de nobreaks nos equipamentos que suportam operações críticas de alta disponibilidade. O cabeamento de energia, telecomunicações e redes deve ser protegido contra acesso não autorizado e danos intencionais ou acidentais.

Equipamentos que processam ou armazenam informações críticas para a empresa devem ser protegidos contra roubo e perda, e as instalações/salas de servidores que os abrigam devem contar com mecanismos de segurança física adequados. Antes do descarte, todos os equipamentos que contenham ou possam conter informações críticas devem ser verificados para garantir a remoção segura dessas informações.

Os procedimentos de manutenção e uso de nobreaks estão descritos no POP APO-003. Os procedimentos de inventário e descarte de equipamentos estão descritos no POP ADM-094.

5.9 Transferência de Informações

A transferência de informações dentro da organização deve seguir as diretrizes estabelecidas nesta Política de Segurança da Informação (PSI), garantindo que todos os procedimentos estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e demais normativas aplicáveis.

Regras Gerais:

- A transmissão de informações deve ser realizada apenas por colaboradores devidamente autorizados e exclusivamente para os fins necessários ao cumprimento de suas funções.
- Qualquer dado pessoal ou sensível transferido deve ser protegido contra acessos não autorizados, utilizando sistemas criptografados ou canais seguros para evitar vazamentos ou acessos indevidos.
- Todas as transferências de dados pessoais realizadas internamente ou para terceiros devem ser documentadas, garantindo rastreabilidade e conformidade com os requisitos legais.
- Apenas as informações estritamente necessárias para a execução da tarefa ou projeto devem ser compartilhadas, evitando a transferência de dados excessivos.
- Conforme exigências da Lei Geral da Proteção de Dados, qualquer transferência internacional feita por sistemas e aplicativos devem ser tratadas pelo DPO a fim de mitigar possíveis riscos de vazamentos de dados pessoais.

5.10 Gestão de Incidentes de Segurança da Informação

A Gestão de Incidentes de Segurança da Informação é o conjunto de processos, procedimentos e controles estabelecidos para identificar, gerenciar, analisar e responder a incidentes que possam comprometer a confidencialidade, integridade ou disponibilidade das informações do IBMP.

Para garantir uma resposta rápida e eficaz em caso de incidentes, todos os colaboradores da organização devem estar cientes de como agir em tais situações. O acionamento da equipe de Segurança da Informação deve seguir os seguintes passos:

- Ao identificar um possível incidente (por exemplo, atividades suspeitas, e-mails de phishing, falhas de segurança, perda de dispositivos), o colaborador deve, imediatamente, notificar a equipe de Segurança da Informação.
- A notificação deve ser feita através dos canais de comunicação estabelecidos, como e-mail específico (ti@ibmp.org.br) e via sistema interno de chamados (conforme POP ADM-015).
- Ao relatar um incidente, inclua o máximo de informações possíveis, como data, hora, descrição detalhada do ocorrido, sistemas envolvidos, e qualquer evidência disponível (capturas de tela, logs etc.).
- Não realize tentativas de resolver o problema por conta própria, pois isso pode agravar a situação ou comprometer a integridade das evidências.

- Após a notificação, a equipe de Segurança da Informação irá avaliar a gravidade do incidente e tomar as medidas necessárias para conter o impacto.
- A equipe poderá solicitar informações adicionais ou orientações específicas para os colaboradores envolvidos no incidente.
- Em casos críticos, a Executiva e a alta administração será informada e medidas de contingência poderão ser acionadas para proteger os sistemas e dados da organização.
- A equipe de Segurança da Informação manterá o colaborador informado sobre o andamento da análise e as ações tomadas para mitigar o incidente.
- O colaborador deve seguir as instruções fornecidas e colaborar durante todo o processo de investigação.
- Em caso de vazamento de dados pessoais, a equipe de segurança da informação deverá acionar o DPO ou a área de privacidade do IBMP, para que sejam iniciadas a coleta de evidências e o apoio na comunicação às partes interessadas.

5.11 Gestão de Infraestrutura do Produto

A infraestrutura de TI engloba hardware softwares e sistemas. Existe uma análise para medir o impacto de sistemas/softwares e, os que são considerados com impacto BPx são validados. Os sistemas são inventariados de acordo com o FPOP-VAR-005-01. A infraestrutura de TI deve ser qualificada conforme normas e regulamentos seguidos pelo IBMP, a qualificação envolve planejamento, documentação, gestão de riscos, controles de mudança, auditorias e inspeções, treinamento e capacitação.

5.12 Gestão de Risco

O IBMP faz o gerenciamento de riscos conforme procedimento estabelecido (POP SGQ-024), este documento descreve e padroniza a metodologia para identificação de situações perigosas, implementação, controle e monitoramento de gerenciamento contínuo de riscos em produtos, processos de Fabricação, Projetos em fase de implementação e determinação de criticidade para processos de suporte ou apoio e monitorar eventos com potencial impacto negativo no cumprimento dos objetivos e requisitos aplicáveis.

5.13 Revisão e Melhoria Contínua

A empresa deve revisar regularmente a política de segurança da informação, os controles implementados e as diretrizes para garantir sua adequação contínua e eficácia. As lições aprendidas com incidentes de segurança da informação devem ser utilizadas para melhorar continuamente o sistema de gestão da segurança da informação.

6. Documentos de Referência

GES-001; POP ADM-007; POP ADM-015; POP ADM-047; POP SGQ-024, 009.000042.

7. Itens Revisados

Item	Alteração	Motivo
3.	Excluída definição do CSP; incluída definição do DPO	Encerramento do CSP
5 e 5.9	Retirada menção ao CSP	
6.	Retirado o RI-001	Documento Cancelado

8. Anexos

Anexo 1 – Termo de Ciência e Concordância.

Esta política passa a vigorar a partir de 12 meses a partir da data de sua publicação, considerando a necessidade de revisão dos procedimentos que venham a ser impactados.

9. Fluxo de Aprovação

Elaborado por: Tahany C. da Silva Adur de Oliveira - Tecnologia da Informação - ANALISTA - 30/10/2026 - 12:59:59
Aprovado por: Guilherme Eduardo Cavassin Paes - Tecnologia da Informação - COORDENADOR - 30/10/2026 - 15:19:27
Homologado por: Kalinka Pereira Gonzales - Garantia da Qualidade - ANALISTA - 05/11/2026 - 10:51:31

10. ASSINATURA – DIRETOR PRESIDENTE

Não Aplicável

Anexo 1

TERMO DE CIÊNCIA E CONCORDÂNCIA

Através do presente Instrumento a empresa

_____,

inscrita no CNPJ sob nº _____, declara que recebeu e tem pleno conhecimento do teor da Política de Segurança da Informação. Concorda expressamente com todas as regras inerentes à esta Política de Segurança da Informação e se compromete a cumprir integralmente todas as regras referidas neste documento.

Tendo ciência de que o descumprimento da Política de Segurança da Informação poderá acarretar a extinção do contrato firmado com a Organização e as consequências jurídicas decorrentes da violação.

Curitiba, de de .