# PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## 1. Introdução e Propósito

A presente Política de Segurança da Informação (PSI) estabelece as diretrizes e responsabilidades essenciais para a proteção dos ativos de informação e dados pessoais no âmbito do Ipreville. Fundamentada no reconhecimento de que as informações constituem um patrimônio vital, esta política visa garantir sua guarda adequada e uso controlado, refletindo o firme comprometimento do Instituto com a segurança e a privacidade.

Este documento tem como objetivo principal unificar e aprimorar as diretrizes de segurança da informação e privacidade de dados no Ipreville. Ele substitui e revoga as Políticas publicadas através das Portarias nº 05/2022 (PSTI) e nº 95/2021 (PSI), compilando as disposições contidas nesses documentos anteriores e avançando sobre outros pontos relevantes.

Sua elaboração garante a adequação integral às novas regras e exigências da Lei Geral de Proteção de Dados Pessoais (LGPD), reforçando a conformidade com a legislação vigente.

Dessa forma, esta PSI assegura a integridade, confidencialidade, disponibilidade e autenticidade das informações.

Ela atua em sinergia com os demais documentos atualizados que estão sendo produzidos pelo Ipreville no processo de adequação à LGPD, estando plenamente alinhada à nomeação e às atribuições do Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD), fortalecendo a governança e a segurança jurídica da instituição.

## 2. Objetivos

Os objetivos desta Política de Segurança da Informação são:

a) Preservar Ativos: Proteger os ativos tangíveis e intangíveis do Ipreville, garantindo a integridade, confidencialidade, disponibilidade e autenticidade de todas as informações;

b) Estabelecer Diretrizes: Definir um conjunto de diretrizes, princípios, responsabilidades e procedimentos para a gestão e o uso seguro da informação e dos Recursos de Tecnologia da Informação e Comunicação (TIC);
c) Garantir Conformidade Legal: Assegurar a conformidade com as obrigações legais e regulatórias aplicáveis, em especial a Lei Geral de Proteção de Dados Pessoais (LGPD), minimizando riscos de sanções e processos administrativos ou judiciais;
d) Promover Cultura de Segurança: Fomentar uma cultura interna de segurança da informação e privacidade de dados, por meio da conscientização e capacitação contínua de todos os colaboradores;
e) Definir Responsabilidades: Esclarecer as responsabilidades e os limites de atuação de todos os membros do Ipreville, bem como de terceiros que tenham acesso aos ativos de informação;
f) Gerenciar Riscos: Identificar, avaliar e mitigar riscos relacionados à segurança da informação e privacidade de dados, incluindo a gestão proativa de incidentes;
g) Apoiar o SGSI: Declarar formalmente o comprometimento do Ipreville na promoção de diretrizes estratégicas, responsabilidades, competências e apoio ao Sistema de Gestão de Segurança da Informação (SGSI)

## 3. Abrangência

Esta PSI aplica-se a todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviços que exercem atividades no âmbito do Ipreville, ou que, de qualquer modo, venham a ter acesso a dados ou informações protegidos pela presente política, independentemente de suas atribuições e responsabilidades.

A abrangência se estende a todos os ativos de informação, em qualquer formato (físico ou digital), e a todos os Recursos de TIC de propriedade do Ipreville ou sob sua responsabilidade.

## 4. Definições Importantes

Para a correta interpretação desta PSI e dos demais documentos relacionados à Segurança da Informação e Privacidade, consideram-se as seguintes definições:

a) Acesso Lógico: Acesso à rede de computadores, sistemas e estações de trabalho por meio de autenticação;

b) Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano ao Ipreville;

c) Aplicativos de Comunicação: Conjunto de código e instruções compiladas, executados ou interpretados por um Recurso de Tecnologia da Informação e Comunicação, armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia;

d) Ativo: É qualquer coisa que tenha valor para o Ipreville e precisa ser adequadamente protegido. Pode ser tangível (hardware, software) ou intangível (dados, reputação, imagem, conhecimento);

e) Autenticidade: Garantia de que a informação não foi alvo de mutações ou alterações ao longo do tempo, sendo, portanto, legítima, procedente e fidedigna, e capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu;

f) Backup: Salvaguarda de informações, realizada por meio de reprodução e/ou espelhamento de uma base de arquivos, com a finalidade de possibilitar a plena e imediata recuperação dos dados em caso de incidente com perda dos dados originais ou em caso de necessidade de restauração;

g) Classificação da Informação: Atribuição, por pessoa designada, do grau de sigilo a ser dado para uma informação;

h) Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD): Órgão colegiado responsável por analisar, recomendar e propor políticas e procedimentos relacionados à privacidade e proteção de dados pessoais, subsidiando o Presidente nas decisões estratégicas do Instituto;

i) Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento alheio;

j) Dados Pessoais: Informações relacionadas a pessoa natural identificada ou identificável;

k) Disponibilidade: Garantia de que a informação e os Recursos de Tecnologia da Informação e Comunicação estejam disponíveis sempre que necessário;

l) Dispositivos Móveis: Equipamentos que podem ser facilmente transportados devido à sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexões com a Internet e outros sistemas, redes ou qualquer dispositivo;

m) Dispositivos Removíveis de Armazenamento de Informação: Dispositivos capazes de armazenar informações que podem ser removidas do equipamento, possibilitando a portabilidade dos dados (ex: CD, DVD, pen drive, HD externo);

n) DPO (“Data Protection Officer”) ou Encarregado pelo Tratamento de Dados Pessoais: Pessoa física ou jurídica indicada pelo Ipreville que atua como canal de comunicação entre o Instituto, os titulares dos dados pessoais e a Agência Nacional de Proteção de Dados (ANPD);

o) Firewall: Combinação de hardware e software que isola a rede interna de uma organização da internet em geral, permitindo filtragem de alguns pacotes e bloqueando o que não é autorizado;

p) Identidade Digital: Identificação do servidor ou usuário em ambientes lógicos, composta por nome de usuário (login) e senha ou outros mecanismos de identificação e autenticação (ex: crachá magnético, certificado digital, token, biometria);

q) Incidente de Segurança da Informação e Comunicação: Ocorrência de evento adverso, relacionado à segurança da informação ou à confidencialidade da comunicação, confirmado ou sob suspeita, que leve à perda de um ou mais dos princípios básicos de segurança da informação (confidencialidade, integridade e disponibilidade), ou que de qualquer forma indique possível violação à Política de Segurança da Informação, falha de controles ou situação previamente desconhecida, relevante à segurança da informação;

r) Informação: Conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento,

contidos em qualquer meio, suporte ou formato. Inclui dados pessoais, nos termos da LGPD;

s) Integridade: Garantia de que as informações não sofram alterações, diminuições, supressões ilegítimas, mantendo-se ilesas e íntegras durante todo o seu ciclo de vida;

t) LGPD (Lei Geral de Proteção de Dados Pessoais): Lei nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

u) Plano de Resposta a Incidentes (PRI): Documento que estabelece um guia claro e prático para as ações a serem tomadas em caso de ocorrência ou suspeita de incidentes relacionados à segurança ou à privacidade de dados, visando minimizar impactos e garantir a conformidade;

v) Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC): Hardware, software, serviços de conexão e comunicação ou de infraestrutura física, necessários para criação, registro, armazenamento, manuseio, transporte, compartilhamento e descarte de informações;

w) Risco: Combinação da probabilidade da concretização de uma ameaça (eventual e incerta) e seus potenciais impactos;

x) Segurança da Informação: Proteção contra o uso ou acesso não autorizado à informação, bem como a proteção da navegação do serviço a usuários autorizados, enquanto a integridade e a confidencialidade dessa informação são preservadas. Refere-se à segurança e proteção das informações sob a guarda do Ipreville, independentemente do meio (físico ou digital). Abrange também a infraestrutura, a tecnologia, os processos e os sistemas que permitem o uso seguro e inviolável das informações;

y) SGSI (Sistema de Gestão de Segurança da Informação): Ambiente de gestão corporativo voltado para a segurança da informação que inclui a abordagem organizacional usada para proteger a confiabilidade, a integridade e a disponibilidade das informações. Considera-se SGSI uma estrutura organizacional que compreende políticas, procedimentos, processos e

sistemas, projetada para garantir a segurança, privacidade, conformidade e eficiência no manuseio de dados, incluindo dados pessoais e sensíveis, dentro de uma organização. O objetivo é assegurar a conformidade com leis e regulamentos de proteção de dados, como a LGPD e o Marco Civil da Internet, além de implementar frameworks de Segurança da Informação, como NIST e ISO/IEC 27001;

z) Titular da Unidade Administrativa: Servidor responsável pela coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração de uma informação no âmbito de sua respectiva área;

aa) Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do Ipreville, ou que de qualquer forma viole a presente política de segurança da informação.

## 5. Princípios da Segurança da Informação

A PSI é estruturada com base nos seguintes princípios:

a) Comprometimento de Todos: A segurança da informação é responsabilidade de todos os envolvidos com o Ipreville. Cada indivíduo deve conhecer e cumprir as normas e orientações estabelecidas, zelando pela proteção dos dados e informações;

b) Abordagem Baseada em Riscos: As decisões relativas à segurança da informação são fundamentadas na análise e avaliação dos riscos de descontinuidade das ações do Ipreville, de conformidade, de responsabilidade civil, de danos e perdas financeiras;

c) Confidencialidade, Integridade e Disponibilidade (CID): Estes são os pilares da segurança da informação. A PSI garante que a informação esteja acessível apenas a indivíduos autorizados (Confidencialidade), que sua exatidão e completude sejam mantidas (Integridade), e que ela esteja

disponível sempre que necessário para usuários autorizados (Disponibilidade);

d) Autenticidade e Não Repúdio: Assegurar que a origem e a autoria das informações sejam verificáveis e que as ações realizadas não possam ser negadas por quem as executou;
e) Legalidade e Conformidade: Todas as ações de segurança da informação devem estar em conformidade com as leis, regulamentos e normas internas aplicáveis, em especial a LGPD;
f) Melhoria Contínua: A PSI e seus controles são dinâmicos e devem ser revisados e aprimorados periodicamente, considerando a evolução tecnológica, o surgimento de novas ameaças e as lições aprendidas com incidentes;
g) Transparência: O Ipreville se compromete com a transparência na gestão da segurança da informação e privacidade, especialmente em casos de incidentes que envolvam dados pessoais, conforme exigido pela LGPD.

## 6. Diretrizes Gerais

As seguintes diretrizes gerais devem ser observadas por todos que se relacionam com o Ipreville:

### 6.1. Interpretação e Publicidade

a) Interpretação Restritiva: Esta PSI e seus documentos complementares devem ser interpretados de forma restritiva. Atividades não expressamente tratadas nos normativos só devem ser realizadas após prévia e formal autorização do superior hierárquico imediato do servidor;
b) Divulgação: Esta PSI e seus documentos complementares devem ser amplamente divulgados para todos que se relacionam profissionalmente com o Ipreville, visando a publicidade e a conscientização.

### 6.2. Propriedade e Uso dos Ativos e Informações

a) Propriedade do Ipreville: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades, bem como os demais ativos intangíveis e tangíveis disponibilizados, são de propriedade ou estão sob a responsabilidade e direito de uso exclusivo do Instituto;
b) Uso Profissional Exclusivo: Ativos e informações do Ipreville devem ser utilizados unicamente para fins profissionais, de modo lícito, ético e moral;
c) Manutenção dos Ativos: A gestão e manutenção dos ativos devem atender às recomendações dos fabricantes e desenvolvedores. Qualquer necessidade de manutenção, atualização ou correção de falhas técnicas somente pode ser realizada pela equipe de Tecnologia da Informação (TI), de acordo com o tipo de ativo;
d) Inventário dos Ativos: O Ipreville deve manter um inventário atualizado de hardwares e softwares, sendo a TI responsável pelo seu registro, armazenamento e atualização.

6.3. Classificação e Sigilo da Informação

Todas as informações de propriedade ou sob a responsabilidade do Ipreville devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida, de acordo com a Política de Classificação da Informação do Instituto:

a) Pública: é uma informação do Ipreville ou de seus segurados com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma;
b) Interna: é uma informação exclusiva para processos do Ipreville, sem cunho público e que deve ter seu acesso, por parte de indivíduos externos ao Ipreville, evitado;
c) Confidencial: é uma informação crítica para os servidores do Ipreville ou de seus segurados. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais aos seus servidores e segurados. É sempre restrita a um grupo específico de pessoas, podendo ser este, composto por servidores, segurados e/ou fornecedores;

d) Informação Restrita: é toda informação que pode ser acessada somente por usuários do Ipreville explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos e/ou comprometer a estratégia do Instituto.

É vedada, a qualquer tempo, a revelação de informação de propriedade ou sob a responsabilidade do Ipreville sem a prévia e formal autorização da Diretoria do Instituto, excetuando-se a informação previamente classificada como pública.

6.4. Uso de Dispositivos e Recursos de TIC

a) Dispositivos Móveis Corporativos: O uso de dispositivos móveis fornecidos pelo Ipreville deve ser solicitado pelo Gerente da Área do servidor e aprovado pela Gerência Administrativa e de Tecnologia da Informação, conforme a função e as necessidades do cargo;
b) Uso de Recursos de TIC/Dispositivos Móveis Particulares: Não é permitido o uso de Recursos de TIC/Dispositivos Móveis particulares na execução de qualquer atividade profissional, exceto quando autorizado expressamente pelo Gerente da Área do servidor e aprovado pela Gerência Administrativa e de Tecnologia da Informação;
c) Comunicação de Dados Sensíveis: É expressamente vedada a comunicação de dados pessoais sensíveis (conforme LGPD, especialmente dados de saúde) no interesse do Ipreville através de aparelhos e dispositivos particulares, exceto se autorizado expressa, formal e justificadamente pela Diretoria do Instituto;
d) Repositórios Digitais e Dispositivos Removíveis: É vedado o uso de repositórios digitais, em nuvem ou dispositivos removíveis não autorizados ou não homologados pelo Ipreville para armazenar ou transmitir informações de propriedade ou sob sua responsabilidade;
e) Aplicativos de Comunicação Instantânea: O uso de aplicativos de comunicação instantânea para troca de informações corporativas deve atender às regras estabelecidas pela Segurança da Informação;
f) Mídias Sociais: O uso de mídias sociais para atividades profissionais deve ocorrer somente quando necessário e de forma restrita ao cumprimento das

funções institucionais, exclusivamente por meio dos Recursos de TIC do Ipreville. A gestão de qualquer mídia social por servidor não lhe transfere a posse ou propriedade da conta e dados relacionados;

g) Identidades Digitais: O uso de credenciais ou identidades digitais do Ipreville não transfere a propriedade ou posse destas ao servidor ou usuário. Não é permitida a alteração de senhas e logins de contas de uso compartilhado sem a prévia autorização do Gerente Administrativo e de Tecnologia da Informação.

6.5. Ambientes Lógicos e Físicos

a) Ambientes Lógicos: Os sistemas e Recursos de TIC que suportam os processos e as informações do Ipreville devem ser confiáveis, íntegros, seguros e disponíveis para a execução das atividades profissionais. O Ipreville deve utilizar sistemas de proteção ativos e atualizados;
b) Ambientes Físicos: O Ipreville deve estabelecer perímetros de segurança para proteção de seus ativos, especialmente aqueles que processam ou armazenam informações/ativos críticos, e implementar controles para identificação e registro de acessos.

6.6. Contratação e Desenvolvimento

a) Contratação com Fornecedores: Contratações que envolvam compartilhamento de informações (especialmente dados pessoais) ou concessão de acesso a ambientes/ativos críticos devem ser precedidas por termos de confidencialidade e cláusulas contratuais relacionadas à segurança da informação;
b) Desenvolvimento e Aquisição de Software: O desenvolvimento interno e/ou externo de softwares, bem como aquisições de mercado, devem garantir o cumprimento das regras previstas nesta política.

6.7. Monitoramento, Auditoria e Treinamento

a) Monitoramento: O Ipreville deve monitorar seus ambientes físicos e lógicos para garantir a eficácia dos controles implantados, a proteção do patrimônio,

a reputação e a identificação de eventos ou alertas de incidentes de segurança da informação;

b) Auditoria e Inspeção: O Ipreville pode auditar ou inspecionar os Recursos de TIC em suas dependências ou que interagem com seus ambientes lógicos, atendendo aos princípios da proporcionalidade, razoabilidade e privacidade, sempre que houver fundada suspeita de violação da presente PSI;

c) Compartilhamento de Imagens CFTV: O acesso aos registros de imagens de monitoramento deve ser avaliado e autorizado pelo Gerente Administrativo e de Tecnologia da Informação do Instituto. Qualquer compartilhamento de imagens com terceiros externos dependerá de determinação judicial ou de autorização expressa e formal do Encarregado pelo Tratamento de Dados Pessoais (DPO);

d) Capacitação: O Ipreville deve estabelecer um plano periódico e anual de capacitação para o desenvolvimento e manutenção das habilidades dos servidores sobre segurança da informação e tratamento adequado de dados pessoais.

## 7. Responsabilidades

A segurança da informação é uma responsabilidade compartilhada. As principais responsabilidades são atribuídas da seguinte forma:

### 7.1. De Todos os Usuários e Servidores

É dever de todos, se manterem atualizados e cientes, acerca do conteúdo desta PSI e demais documentos complementares no âmbito do SGSI e cumpri-la integralmente, sob pena de incorrer em sanções civis, penais ou administrativas.

a) Utilizar os ativos do Ipreville com cuidado e zelo, de acordo com as orientações do fabricante, do desenvolvedor e do Instituto;

b) Responder por todo e qualquer acesso aos recursos de TI, bem como pelos efeitos desses acessos efetivados por meio de suas credenciais ou identidades digitais;

c) Zelar pela segurança e sigilo das senhas de acesso às suas identidades digitais, não compartilhando, divulgando ou transferindo a terceiros;
d) Utilizar os ativos e informações da organização somente para fins profissionais, de forma ética e legal, respeitando os direitos e as permissões de uso concedidas;
e) Preservar a integridade, a disponibilidade, a confidencialidade, autenticidade e a legalidade das informações acessadas ou manipuladas, não as utilizando, enviando, transmitindo ou compartilhando indevidamente, em qualquer local ou mídia, inclusive na Internet;
f) Não revelar qualquer informação de propriedade ou sob a responsabilidade do Ipreville a terceiros sem prévia e formal autorização;
g) Reportar formalmente ao seu Gestor quaisquer eventos relativos à violação ou possibilidade de violação de segurança ou atividades suspeitas;
h) Zelar pela segurança e inviolabilidade das senhas de acesso, ou chaves, às quais têm posse seja para ambientes lógicos ou físicos, cumprindo fielmente a política de senhas do Ipreville;
i) Solicitar autorização prévia do supervisor imediato para tratamento de dados pessoais em massa ou em grande escala (ex: cópia de grande quantidade de arquivos físicos ou digitais, download de planilhas com grande quantidade de dados pessoais), observando que tal atividade é permitida apenas para o exercício do trabalho desenvolvido para o Instituto.

7.2. Dos Titulares das Unidades Administrativas

a) Identificar o mau uso dos ativos e adotar prontas medidas corretivas;
b) Solicitar ao Gerente Administrativo e de Tecnologia da Informação a concessão de acesso a usuários sob sua supervisão;
c) Observar e fazer cumprir a presente PSI e demais documentos correlatos ou complementares;
d) Identificar violações ou qualquer ação irregular ou temerária praticada pelos servidores no uso dos recursos de TIC ou de informações do Ipreville e comunicar ao Gestor do servidor e ao Gerente Administrativo e de Tecnologia da Informação;

e) Garantir que os ativos de propriedade ou sob a responsabilidade do Ipreville sejam utilizados com cuidado e de acordo com as orientações do fabricante e do Instituto;
f) Fazer aplicar, após definição com a Gestão de Pessoas, as sanções de violação desta PSI e/ou documentos complementares;
g) Analisar seus processos e Recursos de TIC em intervalos regulares, visando assegurar que estejam devidamente inventariados, com gestores identificados e cientes, e com vulnerabilidades e ameaças de segurança, mapeadas.

7.3. Da Alta Direção (Presidente e Diretores)

a) Fiscalizar o cumprimento das normas estabelecidas na presente política por todos os membros da organização;
b) Analisar e aprovar, ou não, exceções de forma excepcional a esta PSI.

7.4. Do Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD)

O CGPD é o organismo central e a principal instância decisória e deliberativa para a gestão de incidentes de segurança e privacidade de dados, e suas atribuições gerais são:

a) Propor, revisar e recomendar políticas, normas e procedimentos internos de proteção de dados pessoais e privacidade, alinhados à LGPD, incluindo as diretrizes de segurança da tecnologia da informação e acesso a sistemas e dados;
b) Supervisionar e monitorar as atividades de tratamento de dados pessoais realizadas pelo Ipreville, avaliando a conformidade com a LGPD e demais legislações pertinentes;
c) Analisar e recomendar sobre a implementação de medidas de segurança da informação e técnicas de proteção de dados que garantam a confidencialidade, integridade e disponibilidade dos dados pessoais, incluindo regras gerais e específicas de acesso, bloqueios ou liberações para sistemas, sites, downloads e tipos de arquivos externos ao Ipreville, bem como

alterações nas regras de acesso dos usuários do domínio <<ipreville.pmj>> às unidades de rede do Ipreville;

d) Gerenciar e acompanhar o tratamento de solicitações e reclamações dos titulares de dados pessoais, em colaboração com o Encarregado (DPO);

e) Analisar e recomendar sobre a atuação do Encarregado (DPO) em suas interações com a Agência Nacional de Proteção de Dados (ANPD) e titulares de dados, bem como em casos de incidentes de segurança da informação que envolvam dados pessoais, analisando possíveis descumprimentos das políticas relacionadas à proteção e à privacidade de dados pessoais e dados sensíveis, registrados por Relatório de Descumprimento (RD) e propondo ações corretivas e/ou sanções, promovendo o encaminhamento aos órgãos competentes para fins de apuração de responsabilidade e aplicação de sanções, nos termos da Resolução que instituiu o comitê;

f) Orientar e recomendar sobre a realização de Análises de Impacto à Proteção de Dados Pessoais (RIPD/DPIA) e planos de mitigação de riscos, quando necessário;

g) Propor diretrizes para a conscientização e capacitação contínua dos servidores do Ipreville sobre as boas práticas de proteção de dados e privacidade;

h) Promover a melhoria contínua dos processos de tratamento de dados pessoais, da governança de privacidade, da Política de Segurança da Informação do Ipreville e demais normas relacionadas à proteção e à privacidade de dados pessoais e dados sensíveis, analisando as ocorrências registradas através dos RDs e as ações adotadas para sua correção e/ou sanção;

i) Dar suporte para as iniciativas da Gerência Administrativa e de Tecnologia da Informação do Ipreville relacionadas à segurança e proteção de dados;

j) Analisar os incidentes de segurança da informação reportados e submeter relatório para deliberação da Diretoria do Ipreville;

k) Informar imediatamente o Encarregado pelo Tratamento de Dados Pessoais (DPO) sobre a ocorrência de qualquer incidente de segurança da informação

sempre que este comprometer, ou potencialmente comprometer, dados pessoais;

l) Aprovar o procedimento para atendimento às demandas dos titulares de dados pessoais elaborado pelo DPO;

m) Aprovar alterações nesta Política de Segurança da Informação.

7.5. Do Encarregado pelo Tratamento de Dados Pessoais (DPO)

O DPO possui um papel vital na gestão de incidentes, especialmente aqueles que envolvem vazamento de dados pessoais. Suas responsabilidades devem incluir:

a) Atuar como canal de comunicação entre o Ipreville, os titulares de dados e a Agência Nacional de Proteção de Dados (ANPD);

b) Convocar reuniões extraordinárias do Comitê e, na ausência ou falta do Presidente, as reuniões periódicas;

c) Elaborar pareceres técnicos sobre a adequação dos tratamentos de dados pessoais às exigências da LGPD e demais regulamentações, incluindo análises de risco, impacto à privacidade e a avaliação de dano em caso de incidentes;

d) Elaborar dossiê detalhado com a avaliação interna de incidentes de segurança da informação envolvendo dados pessoais, as medidas tomadas e a análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas;

e) Avaliar o nível de dano que um incidente pode ter causado aos titulares de dados pessoais;

f) Realizar a notificação a titulares de dados e à ANPD em casos de incidentes de segurança da informação que possam acarretar risco ou dano relevante aos titulares, conforme recomendação do CGPD;

g) Orientar os demais membros e áreas da organização a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

h) Comunicar-se diretamente com a ANPD e demais órgãos fiscalizadores, no exercício de sua função e nos termos da LGPD e demais normas regulamentadoras, bem como garantir a autonomia necessária para o cumprimento de suas atribuições legais;

i) Fiscalizar o cumprimento das normas estabelecidas na presente política no que se refere à proteção e à privacidade de dados pessoais;
j) Determinar aos setores responsáveis melhorias nos procedimentos relacionados à proteção e à segurança no tratamento de dados pessoais, traçando diretrizes mais protetivas quando se tratar de dados pessoais sensíveis;
k) Manter-se atualizado quanto às tecnologias empregadas pelo Ipreville na proteção e privacidade dos dados pessoais, bem como sugerir ao CGPD a implementação de novas tecnologias sempre que pertinente;
l) Informar o CGPD sempre que identificar qualquer falha de segurança, atual ou potencial, à privacidade, à disponibilidade ou à integridade de dados pessoais;
m) Atualizar periodicamente o Inventário de Dados Pessoais;
n) Sugerir ao CGPD alterações pertinentes nesta PSI, com vistas à proteção e à privacidade dos dados pessoais;
o) Receber reclamações e comunicações dos titulares de dados pessoais;
p) Receber comunicados da ANPD e adotar as devidas providências.

7.6. Do representante da Gerência Administrativa e de Tecnologia da Informação

a) Monitorar o uso dos recursos de TIC da organização e fazer cumprir esta PSI e os documentos complementares por todos os servidores;
b) Identificar e avaliar os riscos relacionados à segurança da informação e propor melhorias e recursos necessários às ações de segurança da informação;
c) Realizar e acompanhar estudos de tecnologias, com o apoio do CGPD, quanto a possíveis impactos na segurança da informação;
d) Elaborar e manter atualizados os documentos que compõem o SGSI, além de submetê-los à aprovação da Diretoria ou do CGPD;
e) Propor, junto do CGPD, normas e procedimentos internos relativos à segurança da informação na organização;
f) Garantir que o andamento e o resultado de mudanças preservem os controles relacionados à disponibilidade, integridade, confidencialidade, autenticidade e

legalidade das informações, sobretudo nos sistemas e na infraestrutura tecnológica;

g) Assegurar que os procedimentos de Gestão da Continuidade do Negócio sejam executados em conformidade com os requisitos de segurança da informação;
h) Auxiliar o Departamento de Recursos Humanos na capacitação dos servidores em segurança de informação;
i) Informar o Encarregado pelo Tratamento de Dados Pessoais, imediatamente, sobre qualquer incidente de segurança de dados que possa afetar a segurança, a privacidade, a integridade ou a disponibilidade de dados pessoais ou dados sensíveis, auxiliando-o no cumprimento das obrigações impostas pela LGPD.

7.7. Do Analista de Tecnologia da Informação

a) Fiscalizar o cumprimento das normas estabelecidas na presente política por todos os membros da organização;
b) Realizar a gestão, manutenção e administração dos Recursos de TIC de propriedade ou sob a responsabilidade da organização;
c) Garantir que todos os Recursos de TIC utilizados atendam às recomendações de seus fabricantes ou desenvolvedores;
d) Definir, analisar e priorizar ações necessárias, balanceando custo e benefício;
e) Realizar o registro e o monitoramento dos acessos aos ambientes lógicos da organização;
f) Informar o Encarregado pelo Tratamento de Dados Pessoais, imediatamente, sobre qualquer incidente de segurança de dados que possa afetar a segurança, a privacidade, a integridade ou a disponibilidade de dados pessoais ou dados pessoais sensíveis, no ambiente lógico, auxiliando-o naquilo que for necessário ao cumprimento das obrigações impostas pela LGPD;
g) Disponibilizar e realizar a gestão das identidades digitais de acesso ao ambiente lógico da organização;

h) Analisar ou auxiliar na análise dos incidentes de segurança da informação reportados;
i) Garantir a rápida recuperação em situações de contingência de seus sistemas e processos que envolvam os Recursos de TIC da organização;
j) Elaborar e/ou manter procedimentos de salvaguarda das informações e dos dados necessários para recuperação dos sistemas da organização;
k) Garantir que não sejam coletados ou tratados dados pessoais sensíveis de maneira desnecessária, bem como que a tais dados sejam dadas proteções maiores no que se referem à segurança e à privacidade.

7.8. Do representante da Consultoria Jurídica

a) Assessorar o Encarregado pelo Tratamento de Dados Pessoais no processo de conformidade legal das atividades de tratamento de Dados Pessoais;
b) Participar, assessorar e orientar, de acordo com os aspectos jurídicos, os processos de contratação e as exigências legislativas relacionadas à segurança da informação;
c) Validar as minutas que devem atender aos controles de segurança da informação aplicáveis aos contratos a serem firmados pela organização junto aos seus fornecedores.

## 8. Controle de Acesso

O controle de acessos é fundamental para a proteção das informações.

a) Acesso Físico: O acesso físico à sala de ativos de TI deve ser controlado e restrito às pessoas autorizadas, através de meios aptos aos controles de autenticação, preferencialmente com controle biométrico de acesso;
b) Acesso Lógico: O acesso aos ativos de Tecnologia da Informação deve ser realizado por meio de credenciais e identidades digitais individuais e exclusivas, garantindo a correta identificação do usuário. É expressamente vedado o compartilhamento de credenciais em qualquer situação. O usuário será responsabilizado por qualquer prejuízo causado pelo mau uso de sua credencial;

c) Credenciais de Administração: A guarda de credenciais com autorização de administração dos sistemas, serviços e elementos ativos de rede ficará a cargo do Analista de Tecnologia da Informação. Sempre que necessário o uso de credenciais de administração por terceiros, o Analista deverá, conforme o caso, providenciar credencial individualizada com privilégios de administração;

d) Rastreabilidade: O Analista de TI deverá, sempre que possível e viável tecnicamente, empregar soluções que procedam ao registro dos acessos aos sistemas, serviços e elementos ativos de rede para assegurar sua rastreabilidade.

e) Gestão de Acessos: O setor de Tecnologia da Informação recepcionará todos os pedidos de concessão ou remoção de direito de acesso aos recursos de TI, contas de e-mail institucional e acesso aos compartilhamentos de rede. Entende-se por movimentação qualquer alteração de vínculo funcional (admissão, desligamento, mudança de lotação, afastamento temporário ou retorno);

f) Vedação de Contas para Não Membros: É vedada a criação de conta de usuário a pessoas que não sejam servidores lotados no Ipreville.

## 9. Uso de Softwares

Softwares e sistemas diferentes daqueles de uso comum e necessários ao bom desenvolvimento das atividades das áreas do Ipreville, distribuídos pelo setor de Tecnologia da Informação junto com o equipamento disponibilizado ao usuário como padrão, deverão ser solicitados à chefia imediata do requisitante que, avaliando a necessidade, encaminhará pedido, acompanhado de justificativa ao Gerente Administrativo e de Tecnologia da Informação.

Somente poderão ser utilizados softwares validados e autorizados pelo setor de Tecnologia da Informação do Ipreville, que deverá verificar a existência do adequado licenciamento ou tomar as providências cabíveis para sua contratação, conforme o caso.

## 10. E-mail Institucional

a) Definição: E-mail institucional é a conta de e-mail criada com o domínio do Ipreville;
b) Documento Institucional: A mensagem de e-mail é considerada documento institucional, podendo o remetente ser responsabilizado por seu conteúdo;
c) Conteúdo Proibido: É vedado divulgar qualquer informação ou material de conteúdo difamatório, obsceno, ameaçador, ofensivo, preconceituoso, libidinoso, pornográfico, profano ou ilegal pelo e-mail institucional. O e-mail institucional não deverá ser utilizado para envio de mensagens que possam ir contra a ética, a moral e os bons costumes;
d) Bloqueio de Extensões: Os bloqueios de extensões nos anexos de e-mail que possam gerar riscos à rede deverão ser definidos pelo setor de Tecnologia da Informação;
e) Acesso Restrito: O acesso às mensagens está restrito ao remetente e ao destinatário, sendo estas invioláveis, salvo por motivo de segurança;
f) Deveres do setor de Tecnologia da Informação:
    a. Configurar o correio eletrônico para enviar e-mail somente após o credenciamento do usuário;
    b. Implementar medidas de filtragem de vírus e spam;
    c. Implementar medidas para limitar o tamanho das caixas postais, definindo cotas, se necessário;
    d. Gerenciar o funcionamento do servidor de correio eletrônico;
    e. Alertar os usuários quanto ao eventual mau funcionamento ou interrupção do serviço de e-mail.

## 11. Internet e Intranet

a) Monitoramento e Bloqueio: O setor de Tecnologia da Informação poderá monitorar os acessos às páginas da Internet, bloqueando o acesso àquelas que possam causar prejuízo à rede, com o intuito de manter a disponibilidade do serviço às atividades do Ipreville. Devem ser bloqueados os acessos a

sites com conteúdo pornográfico, racista, ou qualquer outro que possa ser ofensivo à moral e aos bons costumes;

b) Comunicação de Paralisações: A paralisação programada de serviços de internet, para manutenção preventiva, será previamente comunicada a todos os usuários pelo e-mail institucional;

c) Usos Proibidos da Internet:
    a. Download de programas não autorizados, filmes, jogos, músicas e afins;
    b. Participação em jogos e aplicações de bate-papo, salvo, neste último caso, se relacionadas às atividades desenvolvidas em razão da função institucional.

## 12. Gestão de Incidentes de Segurança e Privacidade

Esta PSI se integra com o Plano de Resposta a Incidentes de Segurança e Privacidade (PRI), que detalha os procedimentos para a gestão de qualquer evento adverso relacionado à segurança da informação e privacidade de dados. O PRI visa garantir uma atuação organizada, eficiente e em conformidade com a legislação vigente, orientando as ações a serem adotadas em caso de ocorrência ou suspeita de incidentes relacionados à segurança ou à privacidade de dados pessoais sob tutela ou custódia do Ipreville.

## 13. Casos Omissos

Os casos omissos serão avaliados pelo Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD) para posterior deliberação. As diretrizes estabelecidas nesta PSI e nas demais normas e procedimentos de segurança não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui um rol enumerativo, sendo obrigação do usuário da informação adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações do Ipreville.

## 14. Sanções

As violações e tentativas de burla desta política, bem como das demais normas e procedimentos de segurança, ou a sua inobservância, serão passíveis de ações corretivas e/ou sanções, nos termos da Resolução do Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD).

Constatada a existência de indícios de irregularidades, incidentes de segurança com danos relevantes ou descumprimento deliberado das normas de proteção de dados e privacidade, o Comitê ou o Encarregado (DPO) deverá promover o imediato encaminhamento dos autos para análise:

a) No caso de infrações cometidas por servidores públicos municipais, o feito será remetido à Comissão Permanente de Acompanhamento e Julgamento, destinada à instrução e julgamento da integralidade dos Processos Administrativos de Apuração de Responsabilidade, seguindo o rito estabelecido pela comissão;
b) No caso de infrações cometidas por empresas contratadas, o processo será encaminhado à unidade gestora do contrato para a aplicação das sanções administrativas cabíveis, observando-se a Lei nº 14.133/2021.

## 15. Revisão e Aprimoramento Contínuo

Esta Política de Segurança da Informação é um documento vivo e deve ser revista e atualizada periodicamente. O Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD) é responsável por garantir que esta PSI e demais normas sejam revisadas e atualizadas sempre que se fizer necessário, não excedendo o período máximo de 12 (doze) meses, visando garantir que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos e atualizados.

As alterações desta PSI e demais normas devem ser aprovadas pelo CGPD e pela Diretoria do Ipreville, devidamente publicadas e efetivamente comunicadas aos servidores e demais partes interessadas. As exceções a esta PSI somente são

admitidas de forma excepcional, devendo ser temporárias e aprovadas previamente pelo CGPD e pela Diretoria do Ipreville para produzirem efeito.

## 16. Disposições Finais

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as Normas e Procedimentos aplicáveis pela organização.

Esta Política de Segurança da Informação entrará em vigor na data de sua publicação, revogando-se as disposições em contrário, especialmente as portarias nº 05/2022 (PSTI) e nº 95/2021, (PSI).