1. OBJETIVO

Estabelecer diretrizes para garantir a efetiva proteção dos dados, informações e conhecimentos gerados, bem como a redução dos riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade, autenticidade das informações na Prodam-SP e a continuidade dos seus negócios.

2. ABRANGÊNCIA

Todos os conselheiros, diretores, empregados, estagiários, aprendizes, fornecedores e prestadores de serviços, bem como toda pessoa física ou jurídica que, de alguma forma, executem atividades funcionais amparadas por contratos ou instrumentos jurídicos e que, para tanto, venham a utilizar ou ter acesso às informações de propriedade da Empresa ou sob sua custódia, em qualquer meio, especialmente, físico ou eletrônico.

3. CONCEITOS

Informação

Conjunto organizado de dados, processados eletronicamente ou não, que podem ser utilizados para produção e transmissão de conhecimento. A informação pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. Seja qual for a forma de apresentação ou o meio pelo qual a informação é compartilhada ou armazenada, é recomendado que seja sempre protegida.

Tratamento

Toda operação realizada com qualquer tipo de informação, com dados da Prodam-SP ou de terceiros, desde coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Segurança da Informação

É a proteção da informação contra vários tipos de ameaças, a fim de garantir a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Comitê de Segurança da Informação (CSI)

Grupo multidisciplinar, ligado à Presidência da Prodam-SP, que reúne representantes de diversas áreas da Empresa, indicados pela Diretoria ou pelo Presidente, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção da Segurança da Informação.
Em sua composição deve necessariamente contar com pelo menos um representante das áreas de Segurança da Informação, Infraestrutura, Negócios, Jurídico, além do Encarregado de Proteção de Dados (DPO) e eventuais indicações da Diretoria. Os membros deverão exercer a função sem prejuízo das suas atribuições e sem gratificação.

Gestor da Informação

É o empregado da Prodam-SP, indicado pelo CSI e aprovado pela Diretoria, para ser responsávelpor um determinado conjunto de informações na Prodam-SP.
O gestor da informação deve ter pleno conhecimento das regras de negócio necessárias para executar as medidas de segurança necessárias.
Estas regras de negócio e medidas de segurança devem ser definidas e validadas pelo proprietário da informação.

Proprietário da Informação

É quem tem a posse legal e define as regras de negócio para o tratamento das informações.

Grupo de Resposta a Incidentes de Segurança (GRIS)

Grupo multidisciplinar composto por técnicos de diversas unidades organizacionais da Prodam- SP, que atua como ponto central para notificações de incidentes de segurança, provendo a coordenação e o apoio no processo de resposta a incidentes. A indicação de seus membros deve ser feita pelo CSI e aprovada pela Diretoria.
Em sua composição deve necessariamente contar com pelo menos um representante das áreas de Segurança da Informação, Infraestrutura, Negócios, Jurídico e Comunicação, além do Encarregado de Proteção de Dados (DPO) e eventuais indicações da Diretoria. Os membros deverão exercer a função sem prejuízo das suas atribuições e sem gratificação.

Termo de Responsabilidade da Política de Segurança da Informação e do Uso dos Recursos de Tecnologia da Informação e Comunicação (TIC) da PRODAM-SP

O Termo de Responsabilidade é um formulário (Formulário 68-522) que tem como objetivo comprovar a ciência do usuário sobre a Política de Segurança da Informação e de suas respectivas normas de apoio, bem como sobre as regras a serem observadas para acesso aos recursos de Tecnologia da Informação e Comunicação (TIC) da Rede Corporativa e as informações da Empresae sob sua custódia, armazenadas ou registradas em qualquer meio, físico ou eletrônico, visando principalmente à manutenção da integridade, confidencialidade e disponibilidade das informações.

4. DIRETRIZES

As diretrizes desta política estão apoiadas nos seguintes princípios:

Integridade – É vedada a manipulação das informações, portanto, são proibidas alterações, supressões e adições de conteúdo nas informações, salvo se expressamente autorizadas pela Empresa.

Confidencialidade – Somente pessoas devidamente autorizadas pela Empresa devem ter acesso à informação.

Disponibilidade – A informação deve estar disponível para as pessoas autorizadas, sempre que necessário ou demandado.

Rastreabilidade – Possibilita acompanhar ou identificar o percurso de um dado ou informação durante um processo: saber onde, como, por quem e quando o dado foi manipulado.

4.1. Proteção da Informação

a) Todas as informações e sistemas de propriedade da Prodam-SP ou sob sua custódia devem ser mantidos em locais protegidos.

b) Deve ser mantido sigilo sobre toda e qualquer informação ou dado a que tiver acesso, não se valendo desse privilégio em benefício próprio ou de terceiros, mesmo depois de findo o vínculo contratual.

c) Não é permitido manter acessíveis ou permitir acesso a pessoas não autorizadas, documentos e informações em qualquer tipo de mídia (eletrônica, impressa ou outros).

d) Todos os dados armazenados em banco de dados em produção somente poderão ser reproduzidos com autorização formal, conforme Instrução Normativa vigente.

e) Todo tráfego de informações entre aplicação e banco de dados deve ser criptografado sempre que possível, e esta regra deve ser prevista durante o desenvolvimento das aplicações.

f) Toda informação pertencente à Prodam-SP ou sob sua custódia deverá possuir mecanismos de proteção e classificação.

g) A classificação dos dados é sempre realizada pelo proprietário da informação, seja ele interno ou externo, levando-se em consideração o disposto na Lei Federal nº 12.527/2011 - Lei de Acesso a Informação (LAI) e Lei Federal nº 13.709/2018 - Lei Geral de Proteção aos Dados Pessoais (LGPD).

h) No mesmo sentido, as informações pertencentes à Prodam-SP ou sob sua custódia serão classificadas segundo grau de sigilo, a ser tratado em política própria.

i) Toda informação de dados pessoais será tratada de acordo com os princípios legais aplicáveis, em especial a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico.

j) O acesso às bases de dados dos sistemas em produção deve ser realizado somente pelas aplicações de produção ou pelos técnicos (Database Administrator – DBA) responsáveis pela manutenção dos bancos de dados, de acordo com os termos vigentes definidos em Instrução Normativa.

k) Todo acesso físico às dependências da Empresa deverá ser previamente autorizado, controlado e monitorado.

l) Para acessar os sistemas da Empresa, os usuários devem fazer uso de senhas/credenciais atribuídas para tal finalidade. Toda senha ou credencial de acesso é pessoal e intransferível e não deve ser divulgada e/ou compartilhada com terceiros.

4.2. Uso dos recursos de Tecnologia da Informação e Comunicação (TIC)

a) Os recursos (hardware e software) mantidos (em qualquer meio) pela Prodam-SP e de sua propriedade somente podem ser utilizados/manipulados por pessoas autorizadas e para uso corporativo.
Todo uso será passível de monitoramento, sem aviso prévio, por parte da Empresa, por pessoal devidamente autorizado, sem se limitar ao acesso à internet, às mensagens recebidas e enviadas e arquivos mantidos sob qualquer forma.
Na condução de monitoramento, a Empresa preservará, de acordo com a legislação vigente, a confidencialidade das informações e a privacidade dos envolvidos.

b) É proibido o uso dos recursos de TIC da Empresa para conduzir negócios estranhos às suas funções profissionais, realizar atividades para fins de ganhos pessoais, propaganda pessoal, angariar ou promover causas religiosas, políticas, comerciais ou qualquer outra atividade incompatível com as atividades profissionais.

c) É proibida a interrupção intencional, interferências, monitoração, bloqueio e desligamento dos recursos da Empresa por pessoas não autorizadas.

d) É proibido o envio, recuperação, acesso, exibição, armazenamento, impressão ou disseminação de materiais ou informações fraudulentas, coercitivas, ameaçadoras, ilícitas, racistas, de conotações sexuais ou obscenas, intimidatórias, difamatórias ou, de qualquer maneira, em desacordo com uma correta conduta profissional.

e) É dever do usuário encerrar a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo.

f) A Empresa deve ser informada sobre qualquer situação que configure violação de sigilo ou que possa colocar em risco a segurança, inclusive se relacionada a terceiros.

4.3. Cláusulas obrigatórias em contratos com terceiros

a) Cláusulas de submissão à Política e Normas de Segurança da Informação

Deve constar das propostas e/ou contratos com fornecedores e prestadores de serviços, cláusula de conformidade com a Política e Normas de Segurança da Informação.

b) Cláusulas de sigilo, proteção e contra espionagem

Em todo contrato firmado com terceiros deverão constar cláusulas para proteção das informações da Prodam-SP - e das informações sob sua custódia - de forma padronizada, a fim de garantir que todos os softwares e hardwares fornecidos serão livresde programas de espionagem (backdoors).

4.4. Descarte de Informações

Toda informação, independentemente da mídia em que estiver armazenada, deverá ser descartada respeitando os prazos legais e conforme acordado com seu proprietário, observadas as políticas e normas vigentes.

Em caso de descarte definitivo, as mídias deverão ser inutilizadas previamente.

Em caso de reutilização, as mídias deverão ser submetidas a processos de limpeza para evitar a recuperação das informações gravadas anteriormente.

4.5. Termo de Responsabilidade da Política de Segurança da Informação e do Uso dos Recursos de Tecnologia da Informação e Comunicação (TIC) da PRODAM-SP

a) Todos os conselheiros, diretores, empregados, estagiários e aprendizes da Prodam-SP deverão tomar ciência e comprometerem-se a respeitar e cumprir, plena e integralmente, as regras consubstanciadas na Política de Segurança da Informação e respectivas normas de utilização de recursos da Empresa.

b) O Termo de Responsabilidade da Política de Segurança da Informação e do Uso dos Recursos de Tecnologia da Informação e Comunicação (TIC) da Prodam-SP deveráser assinado quando do ingresso de conselheiros, diretores, empregados, estagiários e aprendizes e quando houver alteração no texto da Política.

c) Os conselheiros, diretores, empregados, estagiários e aprendizes da Prodam-SP, após ciência da Política e Normas de Segurança da Informação, devem assinar o Formulário 68-522 - “Termo de Responsabilidade pelo Uso de Recursos de TIC” para declarar pleno conhecimento de que estão sujeitos às medidas disciplinares cabíveis, inclusive demissão ou interrupção de outras formas de contratação, independentemente de ações cíveis ou criminais, na forma da legislação em vigor, no caso de vir a ser apurada a pratica de atos ilícitos ou que causem danos de qualquer natureza à Prodam-SP.

d) A Prodam-SP deve manter arquivada no prontuário dos conselheiros, diretores, empregados, estagiários e aprendizes uma via do Formulário 68-522 - “Termo de Responsabilidade pelo Uso de Recursos de TIC”, devidamente assinado pelo usuário.

5. RESPONSABILIDADES

5.1. Diretoria Executiva

Compete à Diretoria Executiva da Prodam-SP:

a) Prover recursos para a implantação da Política de Segurança da Informação;
b) Criar e designar os membros do Comitê de Segurança da Informação;
c) Aprovar a política e as normas de Segurança da Informação e suas revisões; e
d) Aprovar a relação de gestores da informação, indicados pelo CSI.

5.2. Comitê de Segurança da Informação (CSI)

Compete ao CSI:

a) Propor ajustes necessários na estrutura normativa da Segurança da informação;
b) Acompanhar o andamento dos projetos e iniciativas relacionados à Segurança da Informação;
c) Indicar os gestores da informação;
d) Apurar os incidentes de Segurança e subsidiar com informações a aplicação de penalidades;
e) Aprovar a composição do GRIS;
f) Realizar a gestão de riscos relacionados à Segurança da Informação; e
g) Reportar, regularmente, à Diretoria o resultado das suas atividades.

5.3. Grupo de Resposta a Incidentes de Segurança (GRIS)

Compete ao GRIS:

a) Acompanhar ocorrências/incidentes de segurança e propor soluções; e
b) Auxiliar na detecção, solução e prevenção de incidentes de segurança na Empresa.

5.4. Gestor da Informação

Compete ao Gestor da Informação:

a) Fazer a gestão do ativo de informação sob a sua custódia, de forma a garantir a efetividade dos princípios declarados nesta política, quais sejam: confidencialidade, integridade, rastreabilidade e disponibilidade;
b) Interagir junto à entidade proprietária da informação, para que a mesma seja classificada;
c) Manter o controle efetivo do acesso à informação, estabelecer, documentar e fiscalizar as regras de acesso e reavaliar, periodicamente, as autorizações de acesso concedidas;
d) Inventariar todos os ativos de informação sob sua responsabilidade;
e) Manter atualizada a análise de risco do ativo de informação sob sua responsabilidade;
f) Fornecer relatórios ao CSI, quando solicitado, sobre as informações e ativos de informação sob sua responsabilidade;
g) Participar da investigação dos incidentes de segurança relacionados às informações de sua responsabilidade;
h) Sugerir ao CSI procedimentos para proteger os ativos de informação, conforme a classificação realizada pelo proprietário da informação, além da estabelecida pela Política e pelas Normas de Segurança da Informação.

5.5. Proprietário da Informação

Compete ao proprietário da informação:

a) Classificar a informação;
b) Definir políticas de acesso à informação;
c) Aprovar medidas para melhoria da segurança das informações; e
d) Gerenciar regularmente as permissões de acesso às informações.

5.6. Unidades Organizacionais

Compete a todas as Unidades Organizacionais:

a) Cumprir e fazer cumprir a política, normas e procedimentos de Segurança da Informação; e
b) Sugerir ao CSI, de maneira pró-ativa, procedimentos de Segurança da Informação relacionados às suas áreas.

5.7. Gerência Jurídica e de Governança Corporativa (GPJ)

Compete à GPJ da Prodam-SP:

a) Incluir, na análise e elaboração de todos os contratos, claúsulas específicas relacionadas à Política e Normas da Segurança da Informação;
b) Definir e elaborar as cláusulas de sigilo e proteção de dados, de acordo com os critérios da presente política e leis associadas.

5.8. Gerência de Compliance e Gestão de Riscos (GPR)

Compete à GPR verificar a adequada aplicação desta política.

5.9. Gerência de Segurança da Informação (GIT)

Compete à GIT:

a) Projetar, prospectar, implantar e gerir projetos e iniciativas, visando aperfeiçoar a Segurança da informação;
b) Consolidar e prestar informações ao CSI;
c) Indicar a composição do GRIS;
d) Gerir o GRIS.

5.10. Gerência de Gestão e Desenvolvimento de Pessoas (GFG)

A Gerência de Gestão e Desenvolvimento de Pessoas (GFG) deve manter arquivada no prontuário dos diretores, empregados e estagiários uma via do Formulário 68-522 - “Termo de Responsabilidade pelo Uso de Recursos de TIC”, devidamente assinado pelo usuário.

5.11. Usuários

Compete a todos os usuários:

a) Zelar continuamente pela proteção das informações da Empresa e de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;
b) Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
c) Garantir a integridade da informação;
d) Garantir a continuidade dos processos das informações críticas para os negócios da Prodam-SP;
e) Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual e as atividades da Empresa; e
f) Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento da Política e/ou das Normas de Segurança da Informação.

6. VIGÊNCIA, REVISÃO E APROVAÇÃO

Vigência: A partir de sua publicação, com prazo de até 60 dias para implementação de todos os atos necessários.

Revisão: Anual

Responsabilidade	Área
Conteúdo / Revisão	Gerência de Segurança da Informação (GIT)
Elaboração / Manutenção	Gerência de Compliance e Gestão de Riscos (GPR)
Aprovação	Presidência e Conselho de Administração

7. DOCUMENTOS NORMATIVOS VINCULADOS

Associados a esta Política de Segurança da Informação deverão ser publicados normativos específicos que complementam esta documentação.

8. DOCUMENTOS INCORPORADOS E REVOGADOS

Esta Política revoga e substitui o seguinte documento normativo e demais disposições em contrário:

- GTI-PO-001 – Política de Segurança da Informação, versão 1 de 05/05/2020.

9. REFERÊNCIAS LEGAIS E NORMATIVAS

Essa política é apoiada por um conjunto de normativos e procedimentos estabelecidos pela Prodam-SP. A inobservância do disposto nesta Política sujeitará o usuário à aplicação de medidas administrativas, além de outras medidas de ordem trabalhista, civil e criminal, observando, ainda, as

Leis abaixo relacionadas, porém não limitas às mesmas:

- **Lei Federal 8159** de 08 de janeiro de 1991
  Dispõe sobre a Política Nacional de Arquivos Públicos e Privados;

- **Lei Federal nº 9.609** de 19 de fevereiro de 1998
  Dispõe sobre a proteção da Propriedade Intelectual de Programa de Computador;

- **Lei Federal 9610** de 19 de fevereiro de 1998
  Dispõe sobre o Direito Autoral;

- **Lei Federal 9279** de 14 de maio de 1996
  Dispõe sobre a Propriedade Industrial, Marcas e Patentes;

- **Lei Federal 3129** de 14 de outubro de 1982
  Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial;

- **Lei Federal 10406** de 10 de janeiro de 2002
  Institui o Código Civil;

- **Decreto-Lei 2848** de 7 de dezembro de 1940
  Institui o Código Penal;

- **Decreto-Lei 5452** de 1º de maio de 1943
  Consolidação das Leis do Trabalho;

- **Lei Federal Nº 9.296** de 24 de julho de 1996
  Interceptação de comunicação telefônica;

- **Lei Federal 9983** de 14 de julho de 2000
  Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal e prevê outras providências;

- **Lei Federal 12.527** de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI)
  Regula o acesso a Informação;
- **Lei Federal 12.737** de 30 de novembro de 2012
  Tipifica crimes de delitos informáticos;

- **Lei Federal 12.735** de 30 de novembro de 2012
  Tipifica conduta pelo uso de sistema eletrônico, digital ou similares, praticados contra sistemas informatizados;

- **Lei 12.682** de 09 de julho de 2012
  Elaboração e arquivamento de documentos em meios eletromagnéticos;

- **Lei Federal 12.965 de 23 de Abril de 2014**
  Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

- **Lei Federal 13.709 de 14 de Agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)**
  Dispõe sobre a proteção de dados pessoais;

- **Lei Municipal 14.098** de 08 de dezembro de 2005

Proibição de acesso a sites de sexo, drogas, pornografia, pedofilia, violência e armamento;

- **Decreto Municipal 49.914** de 14 de agosto de 2008
  Regulamenta a Lei municipal 14.098/2005, no âmbito da Administração Direta e Indireta do Município de São Paulo;

- **Decreto Municipal nº 53.623** de 12 de dezembro de 2012
  Regulamenta a Lei Federal nº 12.527/2011 – Lei de Acesso à Informação;

- **Decreto Municipal nº 56.519** de 16 de outubro de 2015
  Altera o Decreto **Municipal nº 53.623** de 12 de dezembro de 2012, que regulamenta a Lei de Acesso à Informação;

- **Norma ABNT NBR ISO/IEC 27001:2013**
  Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos.

- **Norma ABNT NBR ISO/IEC 27002:2013**
  Tecnologia da Informação – Técnicas de Segurança – Código de Prática e Controles de Segurança da Informação.

10. DISPOSIÇÕES FINAIS

Não será admitido, em momento algum, a qualquer empregado ou prestador de serviços, alegar o desconhecimento desta política para justificar violações ou falta de cumprimento da mesma.

A inobservância às regras estabelecidas sujeita o infrator e aqueles que com ele colaborarem, a aplicação de medidas disciplinares cabíveis ou previstas nos contratos pelo qual o usuário se vincula à Prodam-SP, sem prejuízo a outras sanções administrativas, cíveis e penais, no caso de eventuais danos e prejuízos causados à Empresa ou a terceiros.

Em caso de violações, a Prodam-SP deverá adotar as medidas necessárias para as devidas sanções.

Situações não previstas e as dúvidas a respeito desta Política deverão ser analisadas pelo Comitê de Segurança da Informação e submetidas à aprovação da Diretoria.

O teor desta Política deve ser levado ao conhecimento de todos os usuários atuais e futuros, que tenham autorização para acesso ou utilizem sistemas informatizados da Prodam-SP.

JOHANN NOGUEIRA DANTAS
Diretor-Presidente

HISTÓRICO DE VERSÕES E ALTERAÇÕES

Versão	Data	Alteração	Origem da Alteração
1.0	05/05/2020	Adequação ao novo modelo de estrutura normativa e revisão de conteúdo.	Migração para a nova estrutura normativa da PRODAM-SP. Incorporação da Norma N-210-010 - Termo de Responsabilidade – Segurança da Informação.
1.1	02/05/2024	Atualização dos nomes e siglas das Unidades Organizacionais, realizada pela Gerência de Compliance e Gestão de Riscos (GPR) em conformidade com a IN-D Nº 005/2022 de 01/09/2022	IN-E 010/2024, INE-E 011/2024 e IN-E 020/2024