1. INTRODUÇÃO

São princípios para o **Sistema de Gestão de Segurança da Informação** a Confidencialidade, a Integridade e a Disponibilidade, conforme norma de mercado para a Segurança da Informação (NBR/ISO 27001-2022). Esses devem ser preservados, controlados e auditados para garantir que as informações estejam protegidas.

2. OBJETIVO

Esta **Política de Segurança da Informação** (PSI), em conjunto com as Políticas Complementares (PC), tem como objetivo estabelecer as diretrizes e critérios para orientar os colaboradores, clientes/associados, parceiros de negócios e fornecedores sobre as melhores práticas a serem adotadas para garantir o atendimento das normas da Segurança da Informação e proteção de dados no ambiente do **OFÍCIO DE REGISTRO DE IMÓVEIS DA COMARCA DE ITAPAGIPE,** doravante denominado apenas como **SERVENTIA**.

A presente PSI visa assegurar:

- A confiabilidade das informações e dados pessoais por meio da preservação da confidencialidade, integridade e disponibilidade dos dados;
- O compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda;
- A participação e o cumprimento das medidas protetivas por todos os colaboradores, clientes/associados, parceiros de negócios e fornecedores em todos os processos que tratem informações;
- A definição dos princípios e diretrizes gerais que visam a preservação da segurança da informação e da proteção de dados pessoais, primando pela legalidade dos processos que amparam a operacionalização e a gestão das atividades;
- O estabelecimento das responsabilidades e limites de atuação da alta direção, colaboradores, prestadores de serviços e parceiros em relação à segurança da informação e proteção de dados pessoais reforçando uma cultura interna entre os envolvidos baseada em integridade e confidencialidade.

3. ABRANGÊNCIA

Esta política se aplica a todos aqueles que exerçam, ainda que transitoriamente, acesso às informações e processos de negócios da serventia.

4. APLICAÇÃO

Esta PSI é um documento com valor jurídico e aplicabilidade imediata e indistinta, a partir da sua publicação, a: alta direção colaboradores, clientes/associados, parceiros de negócios e fornecedores da serventia.

5. DEFINIÇÕES

Para melhor interpretação da presente PSI consideram-se:

- **Usuários:** todos os envolvidos, independente de cargo ocupado, no manuseio da

informação durante as suas atividades diárias;

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável;
- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **Informação:** qualquer conteúdo que tenha ou traga valor para a serventia ou ao profissional para que alcance seu objetivo;
- **Risco:** estabelece a relação entre probabilidade e impacto em uma determinada situação ou atividade. Essa análise possibilitar determinar como devem ser os investimentos em segurança da informação;
- **Ameaça:** elemento externo ou interno capaz de explorar vulnerabilidades existentes no ambiente da serventia, o qual pode ocasionar prejuízo ou dano para o seu ambiente organizacional;
- **Vulnerabilidade:** fragilidade que pode ser explorada por uma ou mais ameaças no ambiente da serventia;
- **Violação**: qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos, políticas e procedimentos operacionais da serventia;
- **Credencial de Acesso:** é a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e biometria;
- **Incidente de Segurança da Informação**: eventos indesejados ou inesperados que possam colocar em risco as informações armazenadas em meio físico ou eletrônico sob a guarda da serventia ou que tenham grande probabilidade de comprometer as operações do seu negócio e ameaçar a segurança da informação;
- **Incidente de Segurança com dados pessoais**: é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, ais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.
- **Classificação da Informação**: processo que compreende a identificação e definição de níveis e critérios de proteção para as informações, de forma a garantir sua confidencialidade, integridade e disponibilidade;
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Integridade**: salvaguarda da exatidão e completeza da informação;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes tempestivamente (no momento da solicitação);
- **Confiabilidade**: recurso relativo à consistência no comportamento e nos resultados desejados;

- **Impacto:** trata das consequências esperadas caso as informações protegidas sejam expostas de forma não autorizada;
- **Probabilidade:** oportunidade de uma vulnerabilidade ser explorada por uma ameaça;
- **Sigilo profissional:** trata da manutenção de segredo para informação valiosa, cujo domínio de divulgação deva ser fechado, ou seja, restrito a um cliente, a uma serventia ou a um grupo, uma vez que a ele é confiada a manipulação da informação;
- **Gestão de Risco**: atividades coordenadas para dirigir e controlar uma serventia em relação ao risco, aplicabilidade de suas políticas de segurança bem como monitoramento e revisão dos riscos;
- **Plano de Continuidade do Negócio**: fornece estratégias para garantir que serviços essenciais ou críticos sejam identificados, para garantir sua preservação após a ocorrência de um desastre e até o retorno da situação normal de funcionamento da serventia. Também prevê quais planos de ação devem ser realizados em cada momento;
- **Comitê de Segurança da Informação (CSI):** é o comitê composto por uma equipe multidisciplinar, cuja principal função está em assessorar a implementação das ações relacionadas à Segurança da Informação, além de avaliar os controles e incidentes de segurança relacionados.

6. DIRETRIZES

As diretrizes e normas referentes à presente PSI são estabelecidas a seguir.

6.1. Interpretação

Esta PSI e seus documentos complementares devem ser interpretados dentro do contexto de uso de informações e recursos de TI. Tudo o que não estiver expressamente permitido apenas poderá ser realizado após prévia autorização do Comitê de Segurança da Informação (CSI), devendo ser levada em consideração a análise de risco e a necessidade do negócio à época de sua solicitação.

6.2. Propriedade

As informações geradas, acessadas, manuseadas, transmitidas, compartilhadas, armazenadas ou descartadas por gestores, colaboradores e terceiros no exercício de suas atividades profissionais com a serventia, bem como os demais recursos tangíveis e intangíveis disponibilizados a esses atores são de sua propriedade exclusiva, as quais devem ser empregadas exclusivamente em atividades de interesse da mesma.

6.3. Proteção da Informação

As informações geradas, adquiridas, armazenadas, processadas, transmitidas e descartadas pela serventia devem ter mecanismos de proteção adequados, de forma a resguardar sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Os mecanismos de proteção devem estar em conformidade com a legislação vigente, e com a versão vigente das normas de Segurança da Informação da ISO 27001 para as informações tratadas pela serventia e da ISO 27701 para informações que evolvam dados pessoais.

6.4. Classificação da Informação

As informações de propriedade ou sob a responsabilidade da serventia, devem ser classificadas de forma a serem protegidas adequadamente, com controles compatíveis em todo o seu ciclo de vida, por meio da implementação de ferramentas e formalização de processos em instrumento específico, nos termos dos Normativos Internos de Segurança da Informação ou legislação prevista para cada tipo de informação por ela tratada.

6.5. Controle de Acesso às Informações

Toda informação utilizada pelas áreas, aplicações e ou sistemas geridos ou sob responsabilidade da serventia, deve ter seu acesso controlado e monitorado, sendo que cada usuário deve ter acesso a apenas o que realmente necessita para execução de suas atividades, sendo vetados os acessos não autorizados dos demais profissionais ao acervo físico e lógico da serventia.

6.6. Privacidade e Proteção de Dados

A serventia respeita a privacidade dos titulares de dados e garante a proteção e segurança dos dados pessoais durante todo o processo de tratamento de seus dados até o seu descarte final, por meios de processos de segurança física e lógica.

6.7. Responsabilidade em relação a Segurança da Informação tratadas

6.7.1. O usuário é responsável pela segurança das informações a que tenha acesso;

6.7.2. Os usuários devem notificar à equipe de Gestão de Segurança ou ao Comitê de Segurança da Informação (CSI) os casos de violação das regras e eventuais falhas de Segurança da Informação ou violação de dados pessoais mediante registro de incidente de segurança;

6.7.3. Os gestores das áreas devem conscientizar usuários, prestadores de serviços, fornecedores com os quais a área tenha contato direto, além de visitantes sobre a importância da Segurança das Informações e proteção dos dados pessoais utilizados pela serventia e do cumprimento ao disposto nesta política.

6.8. Gestão de Continuidade do Negócio

A serventia é responsável por elaborar e manter um plano de continuidade de negócios, de acordo com a sua necessidade ou exigências legais, de forma a reduzir os impactos decorrentes da interrupção de serviços causada por desastres ambientais ou não, bem como falhas da segurança física e lógica. Deve existir para cada situação um plano de continuidade, contendo informações mínimas para recuperação do serviço e forma para manter a integridade das informações sob sua custódia.

6.9. Gestão de Riscos

A serventia é responsável por implementar e manter um processo para análise e gestão dos riscos, objetivando minimizar possíveis impactos sobre as informações tratadas e mantidas em seu ambiente, bem como para novas informações a serem coletadas ou produtos que poderão utilizar informações existentes as quais eram destinadas a outras atividades de tratamento.

O processo de gestão de riscos também deverá avaliar o escopo da infraestrutura que mantém informações sob sua responsabilidade e deve definir plano para os ativos a serem protegidos, bem

como os dados pessoais mantidos.

O processo de gestão de risco deve subsidiar informações para definir e implantar controles para a identificação e tratamento de problemas relacionados à segurança e proteção de dados pessoais.

6.10. Tratamento de Incidentes

Devem ser estabelecidos procedimentos formais para notificação de incidentes de segurança da informação, bem como procedimentos de resposta a incidentes, sendo obrigatória a notificação desses incidentes a todos que possam estar envolvidos.

Para incidentes que envolvam dados pessoais deverão ser estabelecidos procedimentos para avaliação dos riscos e impactos do incidente a necessidade da elaboração de Relatório de Impacto à Proteção de Dados – RIPD, bem como a avaliação sobre a necessidade de notificação do mesmo à Autoridade Nacional de Proteção de Dados – ANPD e aos titulares de dados.

7. COMPETÊNCIAS

7.1. Compete ao Comitê de Segurança da Informação:

- Propor diretrizes e normas de caráter geral, políticas e estratégias em segurança da informação.
- Elaborar o planejamento e gestão da Segurança da Informação e proteção de dados pessoais.
- Elaborar documentos necessários à Segurança da Informação e proteção de dados pessoais.
- Elaborar, divulgar para as partes interessadas, manter e aperfeiçoar os indicadores de Segurança da Informação e proteção de dados pessoais.
- Elaborar, implementar, manter e melhorar o Plano de Continuidade de Negócios.
- Coordenar juntamente com a equipe de Recursos Humanos programas de treinamento e de conscientização em Segurança da Informação e proteção de dados pessoais.
- Analisar os incidentes de Segurança da Informação e recomendar as ações corretivas e preventivas.
- Assegurar que o sistema de gestão da segurança da informação está em conformidade com os requisitos da norma ISO 27001 vigente e à LGPD.
- Relatar o desempenho do sistema de Gestão da Segurança da Informação para a Alta Direção.

7.2. Compete à Alta Direção:

- Aprovar a Política de Segurança da Informação.
- Patrocinar a implementação da Política de Segurança da Informação.
- Apoiar o processo de melhoria contínua do Sistema de Gestão de Segurança da Informação e proteção de dados pessoais.

7.3. Compete ao Departamento de Recursos Humanos:

- Promover, com o envolvimento do Comitê de Segurança da Informação, palestras de

conscientização dos colaboradores em relação à importância da segurança da informação para o negócio da serventia**.**

- Manter o registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações, mediante solicitação à TI.
- Ficará responsável por informar prontamente à TI acerca dos desligamentos e mudança de função dos colaboradores.
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade.
- Elaborar, em parceria com o Comitê de Segurança da Informação, um plano de comunicação e disseminação da Política de Segurança da Informação e proteção de dados pessoais.

8. CONSCIENTIZAÇÃO E CAPACITAÇÃO

Os usuários devem ser instruídos para a correta utilização das informações, dos recursos computacionais, sistemas, aplicações e serviços disponibilizados pela serventia, ela deverá manter um plano de capacitação em segurança da informação e proteção de dados pessoais, voltada aos colaboradores cujas atividades sejam direcionadas correlatas aos assuntos citados anteriormente.

9. PENALIDADES

Violações: Os incidentes de segurança da informação e proteção de dados pessoais identificados como violações devem ser avaliados pela equipe do CSI, a qual fará a avalição sobre o incidente e posteriormente deverá elaborar relatório e, quando possível identificar os responsáveis enviando à área gestora e ao RH para medidas cabíveis, previstas em cláusulas contratuais, normas e políticas dentre outros documentos normativos da serventia. Para os incidentes que envolvam dados pessoais deverá ser avaliada a necessidade de comunicação à ANPD.

Inobservância às normas: A tentativa de transgredir ou burlar as diretrizes e controles estabelecidos nesta PSI e suas complementações, quando constatada, deve ser tratada como uma violação.

10. POLÍTICAS COMPLEMENTARES (PC)

A Política de Segurança da Informação (PSI) no âmbito da serventia está estruturada com as Políticas Complementares indicadas a seguir, que tratam da gestão dos recursos tecnológicos e devem ser atendidas conforme sua especificidade:

10.1. PC01 – Política de Uso de Senhas

Estabelecer critérios para a criação de senhas fortes, proteção dessas senhas, bem como a frequência de suas atualizações.

10.2. PC02 – Política de Uso do Correio Eletrônico

Estabelecer critérios que determinem as exigências mínimas de segurança para uma comunicação através do correio eletrônico institucional.

10.3. PC03 – Política de Resposta a Incidentes de Segurança da Informação

Estabelecer medidas a serem tomadas nos tratamentos de incidentes, envolvendo a segurança das informações. Os Incidentes de Segurança da Informação em eventos podem resultar em perda, dano ou acesso não autorizado às informações.

10.4. PC04 – Política de Classificação da Informação

Estabelecer padrões na determinação de quais informações podem ser divulgadas fora da serventia, bem como ser sensível em relação às informações que não devem ser divulgadas sem a devida autorização.

10.5. PC05 – Política de Aquisição, Desenvolvimento e Manutenção de Sistemas de Informações

Estabelecer as exigências mínimas que devem ser atendidas no desenvolvimento, aquisição e suporte das aplicações sistêmicas.

10.6. PC06 – Política de Uso da Internet

Estabelecer as exigências mínimas de segurança da informação para o uso seguro da Internet.

10.7. PC07 – Política de Acesso Remoto

Estabelecer regras e requisitos para acesso externo à rede da serventia e minimizar o risco potencial para danos que possam resultar do uso não autorizado.

10.8. PC08 – Política de Controle de Acesso

Estabelecer as exigências mínimas na criação de identidades em conformidade com as atividades funcionais e no controle de acesso dos usuários.

10.9. PC09 – Política de Dispositivos Móveis

Estabelecer regras e padrões na utilização e armazenamento dos dispositivos móveis utilizados nas atividades de trabalho da serventia.

10.10. PC10 – Política de Backup Corporativo

Estabelecer padrões para a cópia e restauração, com a finalidade de continuidade e disponibilidade das informações, observando a relevância e criticidade destas.

10.11. PC11 – Política de Combate a Softwares Maliciosos

Estabelecer as exigências mínimas de segurança para a proteção contra softwares maliciosos (vírus, trojan, entre outros).

11. DISPOSIÇÕES GERAIS

Esta Política deverá ser revista no prazo máximo de 12 (doze) meses;

Situações não previstas, dúvidas, informações adicionais e sugestões referentes a esta Política de Segurança da Informação devem ser encaminhadas ao CSI por meio do e-mail csi@registroitapagipe.com.br. O não cumprimento da Política de Segurança da Informação sujeitará o usuário à suspensão temporária ou permanente do acesso aos recursos informacionais do ambiente corporativo.

12. REVISÃO

Esta PSI entra em vigor a partir da aprovação da Alta Direção, RH, Equipe de TI, na data (15/02/2023).

13. DOCUMENTOS DE REFERÊNCIA

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de segurança – Sistemas de Gestão de Segurança da Informação – Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a Gestão da Segurança da Informação;
- ABNT NBR ISO/IEC 27701:2019 – Tecnologia da Informação – Técnicas de segurança – Gestão da privacidade da informação — Requisitos e diretrizes;
- Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018.