Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

PARTE I — POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

1. DISPOSIÇÕES PRELIMINARES

1.1 Objetivo

A presente Política de Segurança da Informação (PSI) tem por finalidade estabelecer diretrizes, responsabilidades e controles destinados a assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade de todas as informações e dados tratados no âmbito desta serventia, em conformidade com o Provimento n.º 213/2026 do Conselho Nacional de Justiça e com a Lei n.º 13.709/2018 (LGPD).

Esta PSI constitui o instrumento normativo central da governança de segurança da informação da serventia e fundamenta, de forma integrada, o Plano de Continuidade de Negócios (PCN) e o Plano de Recuperação de Desastres (PRD), reunidos neste documento único.

1.2 Abrangência

Esta Política aplica-se a:

- Delegatário(a), interino(a) ou interventor(a);
- Colaboradores, prepostos, escreventes e auxiliares;
- Estagiários e jovens aprendizes;
- Prestadores de serviço, fornecedores e técnicos de manutenção com acesso — físico ou remoto — a sistemas, redes, equipamentos ou instalações da serventia;
- Qualquer terceiro que, por vínculo contratual ou funcional, acesse informações ou ativos tecnológicos da serventia.

A aplicação desta Política a fornecedores e prestadores de serviço condiciona-se à existência de cláusula contratual específica ou de Termo de Ciência formal, conforme disciplinado na Seção 12.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

1.3 Base Normativa

Constituem fundamento normativo desta Política:

- Provimento n.º 213/2026 do CNJ e seus Anexos I a V;
- Provimento n.º 149/2023 do CNJ (CNN), com as alterações do Provimento n.º 214/2026;
- Lei Federal n.º 6.015/1973 (Lei de Registros Públicos);
- Lei Federal n.º 8.935/1994 (Lei dos Notários e Registradores);
- Lei Federal n.º 13.709/2018 — LGPD;
- Resolução CD/ANPD n.º 15/2024;
- Normas técnicas ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27701 e NIST Cybersecurity Framework, como referências de boas práticas.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

1.4 Definições Essenciais

Termo	Definição
Alta disponibilidade	Arquitetura com redundância e failover automático para minimizar indisponibilidade não planejada.
Dados críticos	Informações cuja perda, alteração ou indisponibilidade compromete a validade dos atos ou a continuidade do serviço.
Dossiê técnico	Conjunto organizado de evidências documentais que comprovam o cumprimento das exigências do Provimento 213/2026.
Incidente crítico	Evento que compromete relevantemente a disponibilidade, integridade, autenticidade ou continuidade do serviço.
RPO	Recovery Point Objective — perda máxima de dados admissível, medida em tempo retroativo ao incidente.
RTO	Recovery Time Objective — tempo máximo para restabelecimento das operações após incidente.
Tríplice comunicação	Obrigação cumulativa de notificar a Corregedoria, a ANPD e o Juiz Corregedor Permanente, quando o incidente for crítico e envolver dados pessoais com risco relevante.
Vulnerabilidade crítica	Falha técnica com potencial de comprometimento significativo de sistemas ou dados.
PCN	Plano de Continuidade de Negócios — conjunto de procedimentos para manter o serviço em situações de crise.
PRD	Plano de Recuperação de Desastres — conjunto de medidas para restaurar sistemas e dados após incidente grave.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

1.5 Classificação e Parâmetros por Classe

A serventia enquadra-se na seguinte classe, conforme art. 16 do Provimento n.º 213/2026:

Parâmetro	Classe 1 (até R$100k/sem.)	Classe 2 (até R$500k/sem.)	Classe 3 (acima R$500k/sem.)
RPO Máximo	24 horas	12 horas	4 horas
RTO Máximo	24 horas	24 horas	8 horas
Backup completo	Até 72 horas	Até 48 horas	Até 24 horas
Teste de restauração	Anual	Anual	Semestral
Trilha de auditoria	Nível Essencial	Nível Essencial	Nível Intermediário
Pentest	Não obrigatório	A cada 3 anos	A cada 2 anos
Retenção de logs	5 anos	5 anos	5 anos
Implementação inicial (Etapas 1+2)	210 dias	150 dias	90 dias
Implementação integral	36 meses	30 meses	24 meses

ENQUADRAMENTO: Esta serventia está enquadrada na Classe 3. Os parâmetros aplicáveis estão destacados na coluna correspondente acima.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

2. GOVERNANÇA E RESPONSABILIDADES

2.1 Estrutura de Governança

A responsabilidade pelo cumprimento desta PSI e do Provimento n.º 213/2026 é pessoal e indelegável do titular da delegação, ainda que haja terceirização de serviços ou participação em solução coletiva (art. 13, §3.º). A estrutura de governança organiza-se da seguinte forma:

Função	Responsabilidades Principais
Delegatário(a) / Controlador(a) de Dados	Aprovar e publicizar esta PSI; responsabilidade pessoal pelo cumprimento do Provimento; declarações formais de conclusão de etapas; decidir sobre comunicações oficiais em incidentes críticos.
Responsável Técnico Interno (TI)	Implementar e manter os controles técnicos; supervisionar contratos de TI; coordenar a resposta técnica a incidentes; manter dossiê técnico e evidências; garantir backups e testes.
Encarregado(a) de Dados / DPO	Atender direitos dos titulares; orientar colaboradores sobre LGPD; receber comunicações da ANPD; avaliar impacto em dados pessoais em incidentes; participar da avaliação de fornecedores.
Colaboradores e Fornecedores	Cumprir esta PSI e os termos dos contratos; comunicar imediatamente anomalias e suspeitas de incidentes; utilizar recursos apenas para fins funcionais.

2.2 Cadeia de Decisão em Situações de Crise

Ao identificar ou suspeitar de um incidente, qualquer colaborador deve comunicar imediatamente o Responsável Técnico e o DPO, simultaneamente. Estes realizam triagem conjunta, classificam a gravidade e, se o incidente for Crítico ou Alto, acionam imediatamente o CISI e o(a) Delegatário(a). O(A) Delegatário(a) decide sobre comunicações oficiais externas.

2.3 Aprovação, Vigência e Revisão

- Esta PSI entra em vigor na data de sua aprovação pelo(a) Delegatário(a);
- Revisão ordinária: mínimo anual;
- Revisão extraordinária obrigatória: sempre que houver alteração normativa relevante, incidente grave ou mudança significativa de infraestrutura;
- Toda atualização deve ser registrada no controle de versões e comunicada a todos os colaboradores.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

3. CONTROLE DE ACESSO E AUTENTICAÇÃO

3.1 Regras Gerais

- Todo acesso a sistemas, bancos de dados e funcionalidades críticas deve ser feito com credenciais individualizadas e intransferíveis;
- É vedado o uso de credenciais genéricas, compartilhadas ou que impeçam a responsabilização individual;
- Os perfis de acesso seguem o princípio do menor privilégio — cada usuário acessa apenas o necessário para suas funções;
- A Autenticação Multifator (MFA) é obrigatória para acessos administrativos, gestão de sistemas, bancos de dados e funcionalidades críticas;
- Contas técnicas automatizadas são admitidas apenas para integrações sistêmicas, com privilégios segregados, registro auditável e vedação de uso para atos notariais ou registrais diretos;
- Senhas devem ter no mínimo 8 caracteres alfanuméricos com letras maiúsculas, minúsculas e símbolos; não devem ser anotadas ou armazenadas em meios não criptografados.

3.2 Ciclo de Vida dos Acessos

Evento	Procedimento	Responsável	Prazo
Concessão de acesso	Solicitação formal documentada e aprovada pelo Delegatário ou Responsável Técnico	TI + Delegatário	Antes do início das atividades
Revisão periódica de acessos	Verificação de perfis ativos e adequação ao princípio do menor privilégio	TI	Semestral (Classes 2 e 3) / Anual (Classe 1)
Desligamento de colaborador	Revogação imediata de todos os acessos; notificação do gestor de área ao TI	Gestor de Área + TI	Imediata ao desligamento
Perda ou suspeita de comprometimento de credencial	Comunicação imediata ao TI e DPO; bloqueio da conta; investigação	Qualquer colaborador	Imediata

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

4. DIRETRIZES DE USO ACEITÁVEL DE RECURSOS

4.1 Princípio Geral

Todos os equipamentos, sistemas, redes, e demais recursos tecnológicos da serventia destinam-se exclusivamente ao exercício das atividades funcionais. O uso está sujeito a monitoramento contínuo, nos termos das políticas internas e da legislação vigente.

4.2 Rede e Internet

- O acesso à internet será dimensionado conforme o grau de responsabilidade do colaborador;
- São proibidos: acesso a sites maliciosos; downloads de arquivos executáveis não autorizados (.exe, .bat, .vbs, etc.); desabilitar o antivírus; acessar redes sociais, jogos ou conteúdo adulto sem autorização expressa do Delegatário para fins funcionais;
- Boas práticas obrigatórias: evitar sites não seguros (sem HTTPS); reportar anomalias ao TI imediatamente.

4.3 Correio Eletrônico

- O e-mail institucional tem caráter exclusivamente funcional;
- São vedados: envio de conteúdo ilícito, ofensivo, sigiloso sem criptografia, spam ou correntes;
- Arquivos somente podem ser enviados nos formatos autorizados pelo TI;
- Mensagens de remetentes desconhecidos com links ou anexos devem ser reportadas ao TI antes de qualquer interação.

4.4 Estações de Trabalho e Equipamentos

- Equipamentos são de propriedade da serventia e de uso exclusivamente funcional;
- É vedada a instalação de software ou hardware sem autorização do TI;
- O colaborador deve bloquear a tela ao se ausentar e desligar os equipamentos ao término da jornada;
- Impressões com dados pessoais descartadas indevidamente devem ser fragmentadas imediatamente.

4.5 Mídias Removíveis e Dispositivos Pessoais (BYOD – Bring Your Own Device)

- Toda mídia removível deve ser submetida à verificação pelo TI antes de qualquer conexão aos equipamentos da serventia;
- Por padrão, as portas USB encontram-se desabilitadas nas estações de trabalho; a habilitação requer autorização formal;

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

- Dispositivos pessoais não devem ser utilizados para armazenar dados da serventia sem autorização formal e criptografia adequada.

4.6 Inteligência Artificial

- O uso de ferramentas de inteligência artificial deve observar as diretrizes da Resolução n.º 615/2025 do CNJ;
- É vedado inserir dados sigilosos, dados pessoais de terceiros ou informações do acervo registral em ferramentas de IA de uso público sem aprovação do TI e do DPO;
- Regulamentação interna específica sobre uso de IA deve ser definida pelo CISI: [A DEFINIR].

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

5. CRIPTOGRAFIA E PROTEÇÃO DE DADOS

5.1 Requisitos Mínimos de Criptografia

Contexto	Requisito Mínimo	Algoritmos Vedados
Dados em trânsito	TLS 1.2 ou superior (ou equivalente tecnicamente superior)	SSL, TLS 1.0, TLS 1.1
Dados críticos em repouso	AES-256 ou padrão equivalente/superior	DES, 3DES, RC4, MD5
Backups externos/nuvem	Criptografia na origem (AES-256), chave sob custódia exclusiva da serventia	Armazenamento sem criptografia
Assinaturas e certificados	SHA-256 ou superior	MD5, SHA-1

5.2 Gestão de Chaves Criptográficas

- Manter inventário atualizado de todas as chaves e certificados digitais em uso;
- Aplicar segregação de custódia: quem utiliza a chave não deve ser quem a administra;
- Implementar política documentada de rotação e renovação periódica;
- Registrar formalmente todas as operações de geração, renovação e revogação;
- Realizar revisão periódica dos padrões criptográficos adotados, substituindo obrigatoriamente protocolos que se tornem obsoletos ou inseguros.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

6. TRILHAS DE AUDITORIA E LOGS

Os sistemas da serventia devem registrar, de forma contínua e imutável, todas as operações relevantes, assegurando a identificação inequívoca do usuário, data, hora com precisão de segundos, natureza da ação e resultado obtido.

6.1 Requisitos Técnicos

- Logs protegidos contra alteração e exclusão não autorizadas, por mecanismos como WORM, assinatura digital, retention lock ou exportação para ambiente de acesso restrito;
- Sincronização de relógio por fonte confiável (NTP);
- Retenção mínima: 5 anos, independentemente dos prazos de backup;
- Nível mínimo obrigatório: Essencial para Classes 1 e 2; Intermediário para Classe 3 (inclui alterações cadastrais, exportações de dados e tentativas de acesso não autorizado).

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

7. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1 Classificação de Gravidade

Nível	Classificação	Exemplos	Ação / Prazo
1	Crítico	Ransomware; vazamento massivo; indisponibilidade total; comprometimento do acervo	Comunicar à Corregedoria em até 72h (meta: 24h); acionar CISI e Delegatário imediatamente
2	Alto	Indisponibilidade parcial; acesso indevido a dados críticos; falha de controles perimetrais	Registrar; acionar TI e DPO; avaliar comunicação se persistir
3	Médio	Malware contido; tentativas de acesso sem sucesso; falhas em sistemas não finalísticos	Registrar internamente; monitorar evolução
4	Baixo	Alertas informativos; falhas pontuais sem exposição de dados	Registrar internamente

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

7.2 Ciclo de Gestão de Incidentes

Fase	Ação	Responsável	Evidência
1. Identificação	Qualquer colaborador comunica ao TI e DPO simultaneamente	Todo colaborador	Registro inicial: data/hora, sistemas afetados, comunicante
2. Classificação	TI e DPO realizam triagem conjunta por gravidade	TI + DPO	Ficha de triagem com nível de gravidade
3. Contenção	Isolamento de sistemas; bloqueio de acessos; preservação de evidências	TI	Checklist de contenção com timestamps
4. Erradicação	Remoção da causa raiz; correção de vulnerabilidade; revogação de credenciais	TI + Fornecedor	Relatório técnico de erradicação
5. Recuperação	Restauração; validação de integridade por hashes; monitoramento reforçado	TI	Relatório de RTO/RPO obtidos
6. Comunicação	Notificações obrigatórias conforme tabela de comunicações	Delegatário + DPO	Cópias dos comunicados enviados
7. Análise Pós-Incidente	Causa raiz, lições aprendidas, plano de melhorias (até 90 dias)	CISI	Relatório RCA; plano de ação documentado

7.3 Comunicações Obrigatórias

Tipo de Incidente	Corregedoria	ANPD	Juiz Corregedor	Fundamento
Crítico, SEM dados pessoais	SIM — até 72h (meta 24h)	Não	Não	Prov. 213, art. 11, §1.º
Crítico, COM dados pessoais e risco ao titular	SIM — até 72h (meta 24h)	SIM — até 3 dias úteis	SIM	Tríplice comunicação
Alto/Médio/Baixo, SEM dados pessoais	Não obrigatória	Não	Não	—
Alto/Médio/Baixo, COM dados pessoais com risco	Não obrigatória	SIM — até 3 dias úteis	SIM	LGPD + CNN, art. 91

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

A TRÍPLICE COMUNICAÇÃO (Corregedoria + ANPD + Juiz Corregedor) somente se configura quando cumulativamente: (i) o incidente for classificado como Crítico e (ii) envolver dados pessoais com risco ou dano relevante ao titular. As três comunicações são obrigatórias e não se substituem.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

8. GESTÃO DE VULNERABILIDADES

Cenário	Prazo de Tratamento	Ações Obrigatórias
Vulnerabilidade crítica sem exploração ativa	Até 30 dias	Aplicar patch/correção; hardening; validação técnica; registrar no dossiê com data de identificação e encerramento
Vulnerabilidade crítica com exploração ativa ou risco iminente	Contenção imediata, preferencialmente até 72 horas	Bloquear vetor de ataque; desativar exposição; reforçar MFA; monitoramento intensificado; correção definitiva com evidência formal
Componentes EOL (sem suporte do fabricante)	Substituição imediata ou mitigação documentada	Proibido o uso de sistemas operacionais, SGBD ou aplicações em estado End of Life; manter evidência documental de suporte vigente

Todas as vulnerabilidades identificadas devem ter registro formal no dossiê técnico com: data de identificação, classificação de risco, responsável, providências adotadas e data de encerramento.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

9. PROTEÇÃO DE DADOS PESSOAIS — LGPD

9.1 Papel da Serventia e Controlador de Dados

Esta serventia atua como controladora de dados pessoais nos termos do art. 5.º, VI, da Lei n.º 13.709/2018. A responsabilidade pelo tratamento de dados pessoais é pessoal e indelegável do(a) Delegatário(a), mesmo quando houver terceirização de serviços.

9.2 Obrigações Mínimas

- Manter Registro de Operações de Tratamento (ROPA), conforme art. 37 da LGPD e art. 85 do CNN, documentando para cada processo: finalidade, base legal, categorias de dados, medidas de segurança, prazos de retenção e formas de descarte;
- Atender às solicitações dos titulares nos prazos legais (confirmação/acesso: imediato; correção/eliminação: 15 dias; demais: 30 dias prorrogáveis);
- Designar DPO/Encarregado(a) — Classe 3 não está dispensada;
- Comunicar incidentes com dados pessoais à ANPD e ao Juiz Corregedor nos prazos legais;
- Promover treinamento periódico de todos os colaboradores sobre proteção de dados;
- Garantir que contratos com fornecedores contenham cláusulas LGPD obrigatórias (vide Seção 12).

9.3 Direitos dos Titulares

O exercício de direitos pode ser feito por formulário eletrônico, formulário físico ou e-mail do DPO. O DPO atua como intermediário. Cautelas específicas aplicáveis ao contexto registral:

- Dados do fólio real sujeitam-se à legislação registral (art. 14 da Lei n.º 6.015/1973);
- Documentos fornecidos via canal LGPD não possuem fé pública;
- A eliminação de dados não alcança aqueles com base legal em obrigação legal (art. 7.º, II, LGPD).

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

10. PROTEÇÃO FÍSICA DE ATIVOS

- O CPD (Centro de Processamento de Dados) é de acesso restrito, com controle formal de quem pode entrar; visitantes e terceiros devem ser acompanhados;
- Em caso de desligamento de colaborador com acesso ao CPD, a lista de autorizados deve ser imediatamente atualizada;
- Infraestrutura elétrica com aterramento técnico certificado e nobreak (SAI/UPS) com autonomia mínima de 30 minutos para desligamento seguro;
- Ambiente protegido contra incêndio, inundações e variações térmicas;
- Dispositivos removíveis somente com autorização formal; descarte de mídias com procedimento documentado de eliminação segura;
- O CPD deve ser mantido limpo e organizado, sem alimentos, bebidas ou produtos inflamáveis; a entrada ou retirada de equipamentos exige solicitação formal.

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

11. GESTÃO DE FORNECEDORES

11.1 Avaliação Prévia (Due Diligence)

Antes de contratar qualquer fornecedor que acesse sistemas, dados ou instalações da serventia, deve ser realizada avaliação prévia de segurança, nos termos do art. 86 do CNN, com participação do TI e do DPO quando houver tratamento de dados pessoais.

11.2 Cláusulas Contratuais Obrigatórias

Todos os contratos com fornecedores de TI devem conter expressamente:

- Confidencialidade — vedação de divulgação de dados e informações da serventia;
- Reversibilidade integral — devolução completa dos dados ao término contratual;
- Portabilidade em formato interoperável e não proprietário;
- Documentação técnica necessária à migração para outro fornecedor;
- Cooperação em caso de transição de fornecedor;
- Gestão de incidentes de segurança com comunicação imediata à serventia;
- Conformidade integral com a LGPD, incluindo as obrigações de operador de dados.

11.3 Monitoramento Contínuo

- Verificação periódica do cumprimento das obrigações contratuais de segurança;
- Revisão dos contratos sempre que houver mudança relevante de escopo ou ambiente tecnológico;
- Realização de teste documentado de extração integral do acervo para mitigação de dependência estrutural (vide PRD — Seção 23).

Salvador (71) 3052-4104
Salvador (71) 3052-4105
Curitiba (41) 3798-5588
www.itech.net.br
contato@itech.net.br

12. CAPACITAÇÃO E CONSCIENTIZAÇÃO

- Todos os colaboradores participam de treinamento periódico sobre segurança da informação e proteção de dados;
- Novos colaboradores recebem treinamento introdutório antes de iniciar suas atividades e assinam o Termo de Compromisso (Apêndice I);
- Todos os treinamentos devem ser registrados formalmente com data, participantes e conteúdo abordado;
- Registros de capacitação devem ser mantidos no dossiê técnico pelo prazo mínimo de 5 anos.

13. INTEROPERABILIDADE E NEUTRALIDADE TECNOLÓGICA

- Os sistemas devem suportar integração com plataformas do CNJ (e-Notariado, CENSEC, RCPN, Justiça Aberta), assegurando canal seguro, autenticação e logs auditáveis das integrações (art. 19 do Provimento 213/2026);
- Adotar preferencialmente padrões abertos: PDF/A, XML;
- Evitar dependência exclusiva de fornecedor único (vendor lock-in), mantendo cópia independente do acervo e plano formal de portabilidade;
- Adoção de tecnologia distinta da especificada é admitida, desde que demonstrada equivalência funcional.

14. DISPOSIÇÕES FINAIS DA PSI

- Esta PSI entra em vigor na data de sua aprovação;
- O descumprimento das normas desta Política sujeita o infrator a sanções administrativas (advertência, suspensão, demissão por justa causa), responsabilização civil e, conforme o caso, penal;
- Casos omissos serão resolvidos pelo Responsável Técnico com ciência do(a) Delegatário(a);
- Esta Política complementa e não substitui as normas legais e regulamentares aplicáveis;
- O cronograma de implementação progressiva observa as Etapas 1 a 5 do Anexo IV do Provimento 213/2026, conforme prazos da Seção 1.5.