POLÍTICA DE SEGURANÇA DA INFORMAÇÂO

Sumário

POLÍTICA DE SEGURANÇA DA INFORMAÇÂO

1. ASSUNTO/OBJETIVO

Definição das diretrizes básicas da política de segurança da Informação do Tribunal de Justiça do Pará (TJPA).

2. FINALIDADE E ÂMBITO DA APLICAÇÃO

Este manual tem por objetivo informar e estabelecer as diretrizes, parâmetros e orientações estratégicas de Segurança da Informação e, a partir da sua existência, normas técnicas específicas, normas de utilização de recursos de informática, procedimentos operacionais, instruções de trabalho e padrões de segurança, compondo assim, uma Política de Segurança da Informação para a instituição. Atendendo a necessidade de garantia dos meios legais para que os gestores possam administrar a estrutura de segurança da informação aplicada a todos os ambientes, sistemas, pessoas e processos do Poder Judiciário do Pará.

3. UNIDADE GESTORA

Serviço de Segurança e Sistemas Básicos (SSSB)

4. PÚBLICO ALVO

Servidores, magistrados, estagiários e os colaboradores em todas as unidades do TJPA.

5. RELAÇÃO COM OUTROS NORMATIVOS

Não se aplica.

6. REGULAMENTAÇÃO UTILIZADA

Portaria nº 990/2009 – GP;
Portaria n° 1045/2010 – GP.

7. DEFINIÇÕES E CONCEITOS BÁSICOS

Segurança da informação – prática de defender informações contra acesso não autorizado, uso, divulgação, interrupção, modificação, leitura, inspeção, gravação ou destruição. É um termo geral que pode ser usado independentemente do formato dos dados;
Classificação da informação – indica o nível de disponibilidade, integridade e confidencialidade necessário para cada tipo de informação;
Disponibilidade – garante confiabilidade e acesso tempestivo aos dados e recursos para pessoas autorizadas;
Integridade – assegura a exatidão e confiabilidade das informações e sistemas e que qualquer modificação não autorizada seja impedida. Mecanismos de *hardware* e *software* e comunicação devem trabalhar em conjunto para manter e processar os dados corretamente garantindo que os dados cheguem aos seus destinos pretendidos sem alteração inesperada;
Confidencialidade – assevera que o necessário nível de sigilo é aplicado em cada ponto de processamento da informação, impedindo a divulgação não autorizada. O nível de confidencialidade exigido deve ser mantido enquanto os dados residem nos sistemas, transitam na rede e quando chegam ao destino;
Vulnerabilidade – *Software*, *hardware*, processo ou fraqueza humana que pode fornecer um atacante a porta aberta que ele está procurando para entrar em um computador ou rede e obter acesso não autorizado aos recursos do ambiente;

8. FLUXOS, FORMULÁRIOS E ORIENTAÇÕES TÉCNICAS

ANEXO I – ESTRUTURA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TJPA.

9. COMPETÊNCIAS E RESPONSABILIDADES

Competirá à Comissão de Informática e à Secretaria de Informática, a manutenção, atualização e monitoramento periódico destas Diretrizes Básicas, bem como sua complementação por intermédio dos demais instrumentos que compõem a Política de Segurança da Informação do Poder Judiciário do Pará.

A revisão por completo das diretrizes deve ocorrer obrigatoriamente, em período não superior a 1 (um) ano, ou a qualquer tempo, em virtude de demanda importante ou urgente, como por exemplo: incidentes de segurança considerados significativos, novas tecnologias, vulnerabilidades encontradas ou novas necessidades legais ou de mercado.

A aprovação de alterações nas Diretrizes, bem como nas Normas Gerais e específicas, instrumentos que compõem a Política de Segurança da Informação, competirá à Presidência, depois de referendado pela Comissão de Informática.

A Presidência do Tribunal de Justiça do Estado do Pará poderá determinar que eventuais monitoramentos possam ser utilizados em pesquisa para identificação de eventuais tentativas ou mesmo infrações contra a Política de Segurança da Informação do Poder Judiciário do Pará.

10. PROCEDIMENTOS

A Política de Segurança da Informação do Poder Judiciário do Pará será estabelecida por intermédio de Diretrizes Básicas de Segurança da Informação, Normas Gerais para Usuários, Normas Gerais para Técnicos, Normas especificas, Procedimentos Operacionais e Instruções de Trabalho.

10.1 Conteúdo das Diretrizes Básicas de Segurança da Informação:

10.1.1 Propriedade da Informação - Garantir que toda informação gerada, em trânsito e/ou custodiada pelo Poder Judiciário do Pará por meio de tecnologia, procedimentos, pessoas e ambientes é de sua propriedade, e será usada apenas por usuários devidamente autorizados para fins profissionais, no estrito interesse da Instituição.

10.1.2 Proteção de Recursos - Proteger os recursos de Tecnologia da Informação e Comunicações, as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada, garantindo sua confidencialidade, integridade e disponibilidade, considerando níveis para a classificação da informação.

10.1.3 Nível de Segurança - Garantir que na criação de novos serviços internos e externos, a seleção de mecanismos de segurança, a aquisição de bens e contratação de serviços levem em consideração o balanceamento de aspectos tais como riscos, tecnologia, austeridade no gasto, qualidade, velocidade e impacto no negócio.

10.1.4 Utilização de Informações e Recursos - Assegurar que informações e recursos tecnológicos sejam tornados disponíveis para magistrados, servidores e terceiros devidamente autorizados e que sejam utilizados apenas para finalidades lícitas, éticas e administrativamente aprovadas, bem como que suas configurações e parâmetros não sejam

alterados sem aprovação prévia, devendo os usuários serem adequadamente identificados.

10.1.5 Classificação da Informação - Garantir que todas as informações tenham classificação de segurança, colocadas de maneira clara, permitindo que sejam adequadamente protegidas quanto ao seu acesso e uso. A informação e/ou a documentação consideradas de acesso restrito devem ter adequada guarda e armazenamento, assim como aquelas sem utilidade, devem ser destruídas no momento do seu descarte.

10.1.6 Sigilo Profissional - Assegurar que informações e recursos estejam sujeitos às regras referentes ao sigilo profissional, garantindo adequada proteção, por meio de termos de responsabilidade e sigilo, aplicados a magistrados e servidores. E de cláusulas contratuais, aplicadas a terceiros.

10.1.7 Conscientização - Tomar medidas para que magistrados, servidores e terceiros com acesso às informações, ambientes e recursos tecnológicos do Poder Judiciário do Pará, sejam devidamente conscientizados quanto à Segurança da Informação, face às suas responsabilidades e atuação.

10.1.8 Monitoramento - Garantir o monitoramento do tráfego de informações efetuado em ambientes e recursos de Tecnologia de Informação e Comunicações, rastreando e identificando possíveis ocorrências de eventos críticos, no estrito interesse da administração do Poder Judiciário do Pará, obedecendo a legislação aplicável.

10.1.9 Gestão de Ativos - Assegurar a análise periódica dos ativos da informação (bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre, pesquisa, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócios, procedimentos de recuperação, trilhas de auditoria e informações armazenadas) de forma que estejam devidamente inventariados, protegidos, tenham um usuário responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança.

10.1.10 Desenvolvimento, Manutenção e Produção de Sistemas – Assegurar que o desenvolvimento, manutenção, aquisição e adaptação de produtos de mercado e sistemas internos e/ou externos, sejam providos dos requisitos de Segurança necessários para garantir informações confiáveis, íntegras e oportunas.

10.1.11 Documentação de Tecnologia da Informação e Comunicações - Assegurar que os sistemas e procedimentos de Tecnologia da Informação e Comunicações (TIC) do Poder Judiciário do Pará tenham documentação e regras adequadas e suficientes para garantir seu entendimento e recuperação em casos de contingências.

10.1.12 Gerenciamento das Operações e Comunicações - Garantir a operação segura e corrente dos recursos do processamento da informação por intermédio da implementação de controles internos de segurança considerando as pessoas, procedimentos, ambientes e tecnologia.

10.1.13 Terceirização ou Prestação de Serviços - Manter nível de segurança da informação adequado, quanto aos aspectos desta política, naquilo que se refere a responsabilidade pelos procedimentos, sistemas e recursos, terceirizados no todo ou em parte, promovendo auditorias periódicas, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

10.1.14 Segurança de Pessoas, Segurança Física e do Ambiente de Tecnologia da Informação e Comunicações - Prover mecanismos para que magistrados, servidores, terceiros e visitantes disponham de segurança adequada no que se refere ao acesso e uso de recursos e ambientes físicos relacionados a Tecnologia da Informação e Comunicações.

10.1.15 Continuidade das Atividades - Garantir a continuidade das atividades do Poder Judiciário do Pará, reduzindo a um período aceitável e factível, a interrupção causada por desastres ou falhas de segurança, por intermédio da combinação de ações de administração de crises, prevenção e recuperação dos serviços.

10.1.16 Prevenção e Resposta a Incidentes - Assegurar que medidas preventivas sejam tomadas com o objetivo de diminuir o risco de ocorrência de fraudes e/ou incidentes que comprometam a segurança da informação, devendo existir canal de comunicação adequado para esse fim.

10.1.17 Administração da Segurança da Informação - Assegurar que a administração da segurança da informação do Poder Judiciário do Pará seja feita pela Presidência, por intermédio de área especifica, com responsabilidades de estabelecer, implementar, manter e coordenar a elaboração e revisão da Política de Segurança da Informação, bem como avaliar e analisar assuntos a ela pertinentes.

10.1.18 Conformidade - Garantir o cumprimento das leis, regulamentos e normas que regem as atividades do Poder Judiciário do Pará, de forma a obter máxima aderência aos instrumentos legais e normativos, garantindo que os requisitos de segurança sejam cumpridos.

10.1.19 Alegação de Desconhecimento - Esclarecer aos usuários de informações, serviços, ambientes e recursos tecnológicos, que não é dado o direito de alegação de desconhecimento desta Política de Segurança da Informação. Visto que a mesma é amplamente divulgada no âmbito interno da organização.

10.1.20 Sanções - Garantir que a não observância dos preceitos deste documento implicará na aplicação de sanções administrativas previstas nas normas internas do Poder Judiciário do Pará, nas cláusulas de responsabilidade e sigilo, e outros preceitos legais pertinentes, pactuadas em contratos, declarações ou termos de responsabilidade, sem prejuízo de responsabilização pecuniária, quando cabível. Em se tratando de magistrado e servidor o ressarcimento do prejuízo não eximirá da penalidade disciplinar cabível. Tratando-se de crime, serão os fatos levados ao conhecimento da autoridade policial, para instauração do respectivo inquérito, sem prejuízo das medidas de natureza cível.

11. RELATÓRIOS GERENCIAIS E INDICADORES

Não se aplica

12. CONSIDERAÇÕES FINAIS

Este normativo deve ser atualizado sempre que houver alteração nos procedimentos ou na ferramenta a ser utilizada. Demais esclarecimentos devem ser dirigidos ao Serviço de Segurança e Sistemas Básicos.

ANEXO I – ESTRUTURA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO TJPA