

Atos da Presidência

DECRETO JUDICIÁRIO Nº 631/2016

Dispõe sobre a Política de Segurança de Tecnologia da Informação, no âmbito do Poder Judiciário do Estado do Paraná, e estabelece competências administrativas aos seus órgãos integrantes.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ, no uso das atribuições que lhe são conferidas por lei, considerando a necessidade de regulamentar a Política de Segurança de Tecnologia da Informação do Poder Judiciário do Estado do Paraná e tendo em vista a proposta técnica apresentada pelo Departamento de Tecnologia da Informação e Comunicação, constante do SEI nº 0063818-25.2015.8.16.6000;

R E S O L V E :

CAPÍTULO I

DAS DISPOSIÇÕES INICIAIS

Art. 1. A Política de Segurança de Tecnologia da Informação - PSTI - do Poder Judiciário do Estado do Paraná é regida pelo presente Decreto, juntamente com as demais normas e procedimentos internos deste Egrégio Tribunal e se aplica a todas suas unidades.

Art. 2. A PSTI, como parte do plano estratégico, objetiva instituir responsabilidades e diretrizes corporativas para a proteção dos ativos de Tecnologia da Informação e a prevenção de responsabilidade legal para todas as autoridades judiciais, servidores e usuários do Poder Judiciário do Estado do Paraná.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3. Para efeito da PSTI, fica estabelecido o significado dos seguintes termos e expressões:

I - Agente Público: aquele que, por força de lei, contrato ou qualquer ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual, ainda que sem retribuição financeira, ao Poder Judiciário do Estado do Paraná;

II - Ameaça: conjunto de fatores internos ou externos capaz de provocar um incidente, que pode resultar em dano para um ativo do Poder Judiciário do Estado do Paraná;

III - Ativo: tudo aquilo que, ligado a Tecnologia da Informação, tem valor tangível ou intangível para o Poder Judiciário do Estado do Paraná, tais como dados, informação, softwares, equipamentos, instalações, serviços, pessoas e imagem institucional;

IV - Autenticidade: propriedade que assegura a veracidade dos dados ou informações, tanto na origem quanto no destino, permitindo a identificação do emissor e do equipamento utilizado, quando for o caso;

V - Comitê de Segurança de Tecnologia da Informação: grupo multidisciplinar formado por magistrados e representantes de áreas do Tribunal de Justiça do Estado do Paraná com a responsabilidade de apreciar, assessorar e aprovar a implementação das ações de segurança da informação, observado o disposto no art. 9º, inciso IV deste Decreto;

VI - Confidencialidade: propriedade que garante acesso à informação somente a pessoas autorizadas;

VII - Criticidade: grau de importância do ativo para a continuidade das atividades e serviços do Poder Judiciário do Estado do Paraná

VIII - Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IX - Incidente de segurança: evento adverso, confirmado ou sob suspeita, relacionado à segurança das autoridades judiciais, da informação ou dos sistemas de computação ou das redes de computadores;

X - Integridade: propriedade de salvaguarda da inviolabilidade do conteúdo da informação na origem, no trânsito e no destino;

XI - Resiliência: capacidade de enfrentamento ágil de situações inesperadas e de superação das adversidades para restabelecer processo de normalidade;

XII - Usuário: todo aquele que está autorizado a obter acesso a informações e sistemas;

XIII - Vulnerabilidade: conjunto de fatores internos ou externos passivo de exploração, com risco de ocorrência de evento adverso indesejado, que pode resultar em danos aos ativos do Poder Judiciário do Estado do Paraná;

XIV - Rastreabilidade: Capacidade de recuperar o histórico dos acessos realizados à informação para fins de auditoria ou investigação;

XV - Norma: instrumentos de apoio para regular atos, padrões e regras, a fim de garantir a aplicabilidade de recursos para o alcance dos atributos da segurança da informação (confidencialidade, integridade, disponibilidade);

XVI - Procedimento: instrumentos de apoio necessários de como proceder para garantir a aplicabilidade de recursos para o alcance dos atributos da segurança da informação (confidencialidade, integridade, disponibilidade).

CAPÍTULO III

DOS OBJETIVOS DA POLÍTICA

Do Objeto Geral

Art. 4. A presente Política tem por objetivo geral estabelecer diretrizes e normas de apoio necessário para assegurar o sigilo, a integridade, a autenticidade e a disponibilidade de dados, informações e conhecimentos no âmbito do Poder Judiciário do Estado do Paraná, de modo a resguardar a legitimidade de sua atuação e contribuir para o cumprimento de suas atribuições legais.

Dos Objetivos Específicos

Art. 5. São objetivos específicos da Política de Segurança de Tecnologia da PSTI:

I - dotar o Poder Judiciário do Estado do Paraná de instrumentos normativos e organizacionais necessários à efetiva implementação da Política de Segurança da Tecnologia da Informação;

II - orientar a adoção de mecanismos, medidas e procedimentos de proteção a dados, informações e conhecimentos relativos à privacidade das pessoas, ao interesse institucional e aos direitos de propriedade intelectual;

III - nortear a adoção de mecanismos, medidas e procedimentos internos para que o acesso a dados e informações sensíveis e sigilosos seja permitido apenas a pessoas e órgãos autorizados, respeitando a legislação vigente;

IV - subsidiar ações voltadas à salvaguarda da exatidão e integridade de dados, informações e conhecimentos, bem como dos métodos de trabalho;

V - direcionar a adoção de medidas que assegurem a disponibilidade de dados, informações, conhecimentos e ativos associados às pessoas e órgãos autorizados;

VI - orientar as ações permanentes de conscientização, capacitação e educação sobre a importância da proteção de dados, informações e conhecimentos, com o propósito de internalizar o compromisso com a segurança da informação.

CAPÍTULO IV

DOS PRINCÍPIOS E DAS DIRETRIZES DA POLÍTICA

Art. 6. Além dos princípios aplicáveis à Administração Pública em geral, a implementação e o cumprimento da Política de que trata esta Resolução atenderão às regras de sigilo e aos princípios de integridade, disponibilidade e autenticidade.

Art. 7. São diretrizes da Política de Segurança da Tecnologia da Informação:

I - a definição de procedimentos e níveis de acesso a dados, informações e conhecimentos no âmbito do Poder Judiciário do Estado do Paraná, segundo a necessidade de conhecer e, quando for o caso, mediante credencial de segurança;

II - a adoção de critérios e procedimentos relacionados à distribuição e ao uso dos bens e ativos do Poder Judiciário do Estado do Paraná;

III - a garantia de que todos os privilégios de acesso a ativos sejam devidamente revisados, modificados ou revogados periodicamente ou quando cessadas as atividades do agente público;

IV - o estabelecimento de normas, padrões e procedimentos necessários ao controle de acesso e à proteção dos agentes públicos e dos ativos do Poder Judiciário do Estado do Paraná;

V - o estabelecimento de normas relativas ao desenvolvimento e à implementação dos Sistemas de Informação, com vistas a garantir a sua interoperabilidade e a obtenção dos níveis de segurança desejados;

VI - o desenvolvimento e a implementação de programas de conscientização e capacitação sobre segurança da informação;

VII - o levantamento de riscos junto com o desenvolvimento e a implementação de planos de contingência e continuidade de negócios;

VIII - o estabelecimento de medidas e procedimentos de proteção contra falhas e danos que possam comprometer as atribuições do Poder Judiciário do Estado do Paraná.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 8. Será instituído, por ato do Presidente do Tribunal de Justiça, o Comitê de Segurança de Tecnologia da Informação, composto:

I - pelo Desembargador Gestor da Tecnologia da Informação, que presidirá o Comitê;

II - por um Juiz Auxiliar da Presidência;

III - por um Juiz Auxiliar da Corregedoria;

IV - pelo Diretor-Geral;

V - pelo Diretor do Departamento de Tecnologia da Informação - DTIC.

Art. 9. Compete ao Comitê de Segurança de Tecnologia da Informação garantir a implementação da Política de Segurança de Tecnologia da Informação, segundo os objetivos, os princípios e as diretrizes estabelecidos neste Decreto, bem como:

I - propor e acompanhar planos de ação para aplicação desta política;

II - propor campanhas de conscientização dos usuários quanto a esta política;

III - dirimir as dúvidas e deliberar questões não contempladas pela política, bem como propor alterações;

IV - deliberar sobre as propostas de normas apresentadas pelo Departamento de Tecnologia da Informação - DTIC, que serão submetidas à aprovação do Presidente do Tribunal de Justiça, sob a forma de instrução normativa, ressalvada a competência do Órgão Especial desta Corte.

Parágrafo único: O Comitê poderá aprovar cartilhas para orientar os usuários na utilização e no acesso aos sistemas de informática.

Art. 10. Compete ao Departamento de Tecnologia da Informação - DTIC - elaborar, propor e submeter normas para os ativos de tecnologia da informação, tais como e não somente:

I - gerenciamento de Identidade e Controle de acesso lógico;

II - controle de acesso à Internet;

III - utilização do correio eletrônico institucional;

IV - utilização de equipamentos de Tecnologia da Informação;

V - homologação de Software;

VI - inventário de recursos computacionais;

VII - plano de continuidade dos negócios;

VIII - monitoramento e auditoria.

Art. 11. Compete às divisões e assessorias do Departamento de Tecnologia da Informação e Comunicação - DTIC, através da pessoa do seu chefe, elaborar, propor e submeter procedimentos para garantir as aplicações das normas da PSTI.

Art. 12. Compete ao Diretor do Departamento de Tecnologia da Informação e Comunicação - DTIC, deliberar sobre as propostas de procedimentos e dirimir dúvidas sobre os mesmos.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 13. A Política de Segurança de Tecnologia da Informação deve ser revisada e atualizada periodicamente, no máximo, a cada 2 anos.

Art. 14. A Política de Segurança de Tecnologia da Informação deve ser aplicada, no que couber, a terceiros contratados ou conveniados.

Art. 15. Este Decreto entra em vigor na data de sua publicação.

Curitiba, 21 de junho de 2016.

PAULO ROBERTO VASCONCELOS

Desembargador

Presidente do Tribunal de Justiça do Estado do Paraná
