PORTARIA Nº 9699/19

Redefine a Política de Segurança da Informação do Tribunal de Justiça do Estado de São Paulo

O **DESEMBARGADOR PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO**, no uso de suas atribuições legais,

CONSIDERANDO o esforço e o investimento empregado para a Modernização do Tribunal de Justiça do Estado de São Paulo e de sua infraestrutura de tecnologia da Informação e de Comunicações;

CONSIDERANDO a importância, nesse contexto, de se registrar as diretrizes básicas que nortearão a implementação de medidas para a Segurança da Informação do Tribunal de Justiça do Estado de São Paulo;

CONSIDERANDO a necessidade de se redefinir parâmetros e orientações estratégicas de Segurança da Informação e, a partir da sua existência, normas técnicas, de usuários, específicas, procedimentos operacionais, instruções de trabalho e padrões de segurança, compondo, assim, uma Política de Segurança da Informação para a Instituição;

CONSIDERANDO a necessidade de assegurar que os gestores possam realizar o gerenciamento da estrutura de segurança da informação do Tribunal de Justiça de São Paulo, definindo, analisando e priorizando as ações necessárias para alcançar os objetivos estabelecidos para a segurança das informações;

CONSIDERANDO que a Política de Segurança da Informação deve ser aplicada a todos os Ambientes, Sistemas, Pessoas e Processos do Tribunal de Justiça de São Paulo;

CONSIDERANDO a necessidade de as diretrizes gerais da organização estarem em consonância com a Lei n º. 11.419 de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial, e com as melhores práticas de mercado, notadamente, a norma ABNT NBR ISO/IEC 27002:2013 “Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação”;

RESOLVE:

ARTIGO 1º. – O Tribunal de Justiça do Estado de São Paulo redefine sua Política de Segurança da Informação, objetivando assegurar que as informações e seus ativos, possuídos ou custodiados, serão estabelecidos, protegidos e utilizados de forma a garantir sua confidencialidade, integridade e disponibilidade, de acordo com a lei, a ética e a confiança da comunidade.

Parágrafo Único - A Política de Segurança da Informação do Tribunal de Justiça de São Paulo (TJSP) será estabelecida por intermédio de Diretrizes Básicas de Segurança da Informação, Normas Gerais para Usuários, Normas Gerais para Técnicos, Normas Específicas, Procedimentos Operacionais e Instruções de Trabalho.

ARTIGO 2º. – As Diretrizes Básicas de Segurança da Informação do TJSP visam:

I. Propriedade da Informação – Garantir que toda informação gerada, em trânsito e/ou custodiada pelo TJSP por meio de tecnologia, procedimentos, pessoas e ambientes, é de sua propriedade, e seja utilizada por usuários devidamente autorizados para fins profissionais, no estrito interesse da Instituição.

II. Proteção de Recursos – Proteger os recursos de tecnologia da informação e comunicação, as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada pelo TJSP, garantindo sua confidencialidade, integridade e disponibilidade, considerando níveis para a classificação da informação.

III. Segurança em Recursos Humanos - Assegurar que magistrados, servidores e partes externas entendem as suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados, bem como estejam conscientes e cumprem as suas responsabilidades pela Segurança da Informação.

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

V. Utilização de Informações e Recursos – Assegurar que informações e recursos sejam disponibilizados para magistrados, servidores e terceiros devidamente autorizados, e que sejam utilizados apenas para as finalidades lícitas, éticas e administrativamente aprovadas e devidamente autorizadas pelo TJSP, bem como que suas configurações não sejam alteradas sem aprovação prévia, sendo os usuários adequadamente identificados.

VI. Senhas e Autenticação – Estabelecer requisitos de controle, fornecimento, uso, proteção e substituição de senhas de acesso a sistemas, seja pelos usuários finais ou mesmo pelos usuários de instalação e manutenção (administradores) dos sistemas.

VII. Classificação e Tratamento 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 as sem utilidade devem ser destruídas no momento do seu descarte.

VIII. Criptografia – Assegurar o uso efetivo e adequado da Criptografia para proteger a confidencialidade, autenticidades e/ou a integridade das informações classificadas como críticas/confidenciais, de acordo com os padrões definidos pelo TJSP.

IX. Sigilo Profissional – Assegurar que informações e recursos estejam sujeitos às regras referentes ao sigilo profissional, garantindo adequada proteção, considerando as cláusulas contratuais (terceiros) e os termos de responsabilidade e sigilo (servidores).

X. Conscientização – Assegurar que magistrados, servidores e terceiros com acesso às informações, ambientes e recursos do TJSP, sejam devidamente conscientizados quanto à Segurança da Informação, face às suas responsabilidades e atuação.

XI. Monitoramento – Garantir o monitoramento do tráfego efetuado em ambientes e recursos de Tecnologia de Informação, rastreando eventos críticos e evidenciando possíveis ocorrências, dando ampla e geral divulgação dessa atividade e da possibilidade de uso desse recurso em casos de incidentes.

XII. Gestão de Ativos – Assegurar a análise periódica dos ativos da informação, de forma que estejam devidamente inventariados, protegidos, tenham um proprietário responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança. Os ativos devem possuir cuidados adequados à manutenção de sua existência junto a Instituição, independentemente da existência de solução de continuidade.

XIII. Desenvolvimento, Manutenção e Aquisição de Sistemas – Assegurar que o desenvolvimento, a manutenção de sistemas internos e/ou externos, sistemas e produtos adquiridos no mercado e customizados atendam a requisitos de segurança necessários para garantir informações confiáveis, íntegras e oportunas em todo o ciclo de vida da informação nesta Instituição.

XIV. Documentação de Tecnologia da Informação e Comunicação – Assegurar que os sistemas, equipamentos e procedimentos de Tecnologia da Informação e Comunicação (TIC) do Tribunal de Justiça do Estado de São Paulo tenham documentação e regras adequadas e suficientes para garantir seu entendimento e recuperação em casos de contingências.

XV. Gerenciamentos das Operações e Comunicação – Garantir a operação segura e corrente dos recursos do processamento e transporte da informação e dos negócios em geral por intermédio da implementação de controles internos e de requisitos de segurança considerando as variáveis: pessoas, procedimentos, ambientes e tecnologia.

XVI. Terceirização ou Prestação de Serviços – Manter nível de segurança da informação adequado, quanto aos aspectos desta política, quando a responsabilidade pelos procedimentos, sistemas e recursos, ou mesmo parte deles, for terceirizada para outra entidade, provendo auditorias periódicas, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

XVII. Capacidade – Assegurar que a utilização dos recursos seja monitorada e ajustada, e as projeções sejam feitas para as necessidades de capacidade futura, garantindo o desempenho requerido dos sistemas do TJSP.

XVIII. Vulnerabilidades – Garantir que a Gestão de Vulnerabilidades seja implementada, com o objetivo de identificar as vulnerabilidades existentes ao TJSP. A exposição a estas vulnerabilidades deve ser avaliada e em tempo hábil, devem ser tomadas as medidas apropriadas para lidar com os riscos associados,

XIX. Segurança para Serviços em Nuvem – Assegurar que sistemas e serviços utilizados pelo TJSP que sejam hospedados em provedores de serviços em nuvem atendam a requisitos de segurança estabelecidos por esta Instituição.

XX. Continuidade das Atividades – Garantir a continuidade das atividades do TJSP reduzindo a um período aceitável, a interrupção causada por desastres ou falhas de segurança, por intermédio da combinação de ações de administração de crise, prevenção e recuperação.

XXI. Prevenção e Resposta a Incidentes – Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo medidas preventivas, tratamento e a comunicação sobre fragilidades e eventos de segurança da informação, através de canal de comunicação adequado para esse fim.

XXII. Cópias de Segurança das Informações (backup/restore) – Assegurar que a Instituição possua rotinas estabelecidas e ferramentas adequadas para realização de cópias de segurança de informações em periodicidade adequada para recuperação de dados e sistemas em caso de falhas operacionais e/ou incidentes de segurança, assim como estabelecer diretrizes para sua proteção e retenção.

XXIII. Organização da Segurança da Informação – Assegurar que o gerenciamento da Segurança da Informação no TJSP seja feito pela alta direção da Instituição, por intermédio de área específica com responsabilidades de estabelecer, implementar, manter e coordenar a elaboração e revisão da Política de Segurança da Informação, bem como na avaliação e análise de assuntos a ela pertinentes, e de todos os assuntos referentes à segurança das informações custodiadas pelo TJSP, nos ambientes físicos e tecnológicos, nos procedimentos e pessoas.

XXIV. Conformidade – Garantir o atendimento das leis, regulamentos e normas que regem as atividades do TJSP, de forma a obter absoluto cumprimento destes instrumentos legais e normativos. Além disso, garantir que os requisitos de segurança legais e/ou instituídos sejam cumpridos, assegurando o nível de segurança desejado. Para garantir a efetividade no

atendimento as leis, regulamentos e normas, o TJSP deve promover auditoria interna em intervalos regulares.

XXV. Alegação de Desconhecimento – Esclarecer aos usuários de informações, procedimentos, ambientes e recursos do TJSP, que não é dado o direito de alegação de desconhecimento desta Política de Segurança da Informação, vez que a mesma é amplamente divulgada no âmbito interno da organização, devendo ser seguida em seu conteúdo e forma.

XXVI. Sanções – Garantir que a não observância dos preceitos deste documento implicará na aplicação de sanções administrativas previstas nas normas internas do TJSP, nas cláusulas de responsabilidade e sigilo, e outros preceitos legais pertinentes à situação, pactuadas em contratos, declarações ou termos de responsabilidade, sem prejuízo, se for o caso, da responsabilização pecuniária que lhe for atribuída. 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.

ARTIGO 3º. – Competirá à Secretaria de Tecnologia da Informação e ao Comitê Gestor de Segurança da Informação a manutenção, atualização e monitoramento periódico dessas Diretrizes Básicas, bem como sua complementação por intermédio dos demais instrumentos que compõe a Política de Segurança da Informação do TJSP, conforme Parágrafo Único do Artigo 1 º. desta Portaria.

§ 1º – A revisão por completo das diretrizes deve ocorrer, obrigatoriamente, em período não superior a 02 (dois) anos, ou a qualquer momento, em virtude de demanda competente ou de necessidade urgente, como por exemplo: incidentes de segurança considerados significativos; nova tecnologia e/ou vulnerabilidades encontradas; ou novas necessidades legais e/ou de mercado.

§ 2º – A aprovação das alterações nas Diretrizes, bem como das Normas Gerais e Específicas, instrumentos que compõe a Política de Segurança da Informação, competirá à Presidência, depois de referendado pelo Comitê Gestor de Segurança da Informação.

ARTIGO 4º. – A Presidência do Tribunal de Justiça do Estado de São Paulo poderá determinar que eventuais monitoramentos possam ser utilizados em pesquisa para identificação de possíveis tentativas ou mesmo para a constatação de infrações contra as Políticas de Segurança da Informação do TJSP.

ARTIGO 5º. – Faz parte integrante desta Portaria, o Glossário (Segurança da Informação), elaborado em conjunto pela Secretaria de Tecnologia da Informação e a Módulo Security Solutions.

ARTIGO 6º. – Exceções às Diretrizes estabelecidas nesta Portaria devem ser avaliadas e documentadas conjuntamente pela STI e Assessoria da Presidência para Assuntos de Informática.

ARTIGO 7º. – Esta Portaria entrará em vigor na data de sua publicação, ficando revogada a Portaria nº 7560//2008 e outas disposições em contrário.

REGISTRE-SE. PUBLIQUE-SE. CUMPRA-SE.
São Paulo, 11 de Janeiro de 2019.

MANOEL DE QUEIROZ PEREIRA CALÇAS
Presidente do Tribunal de Justiça