



TRIBUNAL DE JUSTIÇA DO ESTADO DO PARANÁ  
Rua Álvaro Ramos, 157 - Bairro Centro Cívico - CEP 80530-190 - Curitiba - PR - www.tjpr.jus.br

## **DECRETO Nº 8246507 - DGRH-DDAA**

SEI:TJPR Nº 0096656-74.2022.8.16.6000  
SEI:DOC Nº 8246507

### **DECRETO JUDICIÁRIO Nº 560/2022 – P-GP**

**Dispõe sobre a Política de Segurança da Informação-PSI, 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 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 0096656-74.2022.8.16.6000;

**CONSIDERANDO** que o Tribunal produz e recebe informações no exercício de suas funções e competências, legais e regulamentares, e que essas informações devem permanecer disponíveis, íntegras e com seu devido sigilo resguardado;

**CONSIDERANDO** a importância de adotar as boas práticas de temas de Segurança da Informação recomendadas pelas Normas Técnicas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2010, 27005:2011; 27014:2013 e 31.000:2009;

**CONSIDERANDO** o disposto na Lei Federal nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

**CONSIDERANDO** a Resolução nº 370/2021 do CNJ, a qual estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), especificamente em seu art. 38º ao dispor que *“Cada órgão deverá elaborar e aplicar práticas e processos de segurança da informação e proteção de dados a serem adotadas na instituição, conforme disposto na Lei no 13.709/2018 que dispõe sobre a Proteção de Dados Pessoais.”*;

**CONSIDERANDO** o teor da Resolução nº 396/2021 - Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

**DECRETA:**

## **CAPÍTULO I**

### **DAS DISPOSIÇÕES GERAIS**

**Art. 1º** Fica instituída a Política de Segurança da Informação - PSI a fim de expandir o alcance das diretrizes, responsabilidades e competências para proteção da informação e prevenção de responsabilidade legal para todas as autoridades judiciais, servidores e usuários do Poder Judiciário do Estado do Paraná.

**Art. 2º** Toda informação documentada e produzida ou custodiada pelo usuário, na realização de atividades do Poder Judiciário do Estado do Paraná, possui valor e deve ser protegida para permitir o uso adequado à consecução dos objetivos institucionais, por meio de atividades operacionais e de negócio, segundo as regras definidas nesta Política de Segurança e demais regulamentações.

**Art. 3º** Para os efeitos desta Resolução e de suas normas será considerado o glossário de termos e definições de Segurança da Informação definido em Portaria, a ser expedida pelo Tribunal de Justiça do Paraná no Portal Institucional.

## **CAPÍTULO II**

## **DOS OBJETIVOS DA POLÍTICA**

**Art. 4º** São objetivos da Política de Segurança da Informação (PSI):

**I** - estabelecer diretrizes e normas de apoio necessárias para assegurar a confidencialidade, integridade, disponibilidade e a autenticidade da informação no âmbito do Poder Judiciário do Estado do Paraná;

**II** - orientar o direcionamento para a implementação e manutenção da Segurança da Informação;

**III** - estabelecer estratégias, responsabilidades e competências, visando à estruturação e a institucionalização da Segurança da Informação no âmbito do Poder Judiciário do Estado do Paraná;

**IV** - orientar a implementação das ações necessárias de conscientização, educação e treinamento em Segurança da Informação e proteção de dados pessoais.

## **CAPÍTULO III**

### **DO ESCOPO**

**Art. 5º** Esta Política de Segurança da Informação é destinada a todos os magistrados, servidores, estagiários, prestadores de serviço, terceiros e quaisquer colaboradores que fazem uso ou tenham acesso aos ativos de informação no âmbito do Poder Judiciário Estadual.

**Art. 6º.** Os destinatários desta Política de Segurança da Informação, mencionados no Art. 5º, são corresponsáveis pela Segurança da Informação, de acordo com os preceitos estabelecidos neste Decreto Judiciário, e têm como deveres:

**I** - conhecer e zelar pelo cumprimento desta Política de Segurança da Informação e demais instrumentos;

**II** - proteger as informações sigilosas e pessoais obtidas em decorrência do exercício de suas atividades;

**III** - preservar o sigilo da identificação de usuário e de senhas de acessos individuais a sistemas de informação ou outros tipos de credenciais de acesso que lhes forem atribuídos;

**VI** - utilizar os ativos sob sua responsabilidade de forma segura e

prudente, em observância ao disposto nesta Política de Segurança da Informação, bem como seus normativos derivados;

**V** - reportar incidente de Segurança da Informação de que tiver conhecimento, utilizando mecanismos e canais disponibilizados pelo Tribunal;

**VI** - participar das campanhas de conscientização e de treinamentos pertinentes aos temas de Segurança da Informação e proteção de dados pessoais, conforme planejamento do Tribunal;

**VII** - apoiar nas ações de implementação da Política de Segurança da Informação em aspectos relacionados às suas competências.

**Parágrafo único.** A Segurança da Informação abrange aspectos tecnológicos, humanos e relacionados ao tratamento das informações no âmbito de cada unidade deste Tribunal.

## **CAPÍTULO IV**

### **DAS DIRETRIZES**

**Art. 7º** A Estrutura relacionada à Segurança da Informação no âmbito do Tribunal de Justiça do Paraná é estabelecida e organizada através dos níveis Estratégico, Tático e Operacional:

**I** - Nível Estratégico: Refere-se à Política de Segurança da Informação, que estabelece diretrizes gerais e princípios básicos do tema, à Política de Gestão de Riscos do Poder Judiciário do Estado do Paraná e à Política de Privacidade e Proteção de Dados Pessoais do TJPR;

**II** - Nível Tático: Refere-se às normas complementares de temas sobre Segurança da Informação, que dispõem de obrigações a serem seguidas, conforme alinhamento das diretrizes desta Política de Segurança da Informação. As normas a serem editadas pelo Tribunal devem contemplar no mínimo os seguintes tópicos específicos:

- a)** gestão de Ativos;
- b)** controle de Acesso à Informação;
- c)** cópias de Segurança (backup);
- d)** incidentes de Segurança da Informação;
- e)** vulnerabilidades e Padrões de Configuração Segura;
- f)** monitoramento de Registros de Atividade (logs);

- g)** continuidade de Serviços Essenciais de TIC;
- h)** desenvolvimento Seguro de Sistemas;
- i)** recursos Criptográficos;
- j)** uso Aceitável de Recursos de TI;
- k)** computação em Nuvem;
- l)** trabalho Remoto;
- m)** proteção e privacidade da informação de identificação pessoal;
- n)** fornecedores e prestadores de serviço;

**III - Nível Operacional:** Relacionados à procedimentos de Segurança da Informação que abrangem fluxos de processos, regras de operação, manuais técnicos que executam as orientações apresentadas nas normas de segurança estabelecidas.

**Art. 8º** Conforme a necessidade e conveniência do Tribunal, poderão ser criados normativos sobre outros temas relacionadas à Segurança da Informação.

## **CAPÍTULO V**

### **ESTRUTURA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO**

**Art. 9º** Deve ser instituído, por ato do Presidente do Tribunal de Justiça, o Comitê de Governança de Segurança da Informação - CGSI, composto:

**I** - pelo Desembargador(a) Gestor da Tecnologia da Informação, que presidirá o Comitê;

**II** - por um Juiz(a) Auxiliar da Presidência;

**III** - por um Juiz(a) Auxiliar da Corregedoria;

**IV** - pelo Secretário(a);

**V** - pelo Diretor(a) do Departamento de Tecnologia da Informação - DTIC;

**VI** - pelo Encarregado(a) de Proteção de Dados Pessoais;

**VII** - pelo Desembargador(a) do Núcleo de Inteligência e Segurança Institucional (NISI);

**VIII** - por membros do Núcleo de Governança, Riscos e Compliance (NGRC) ou o responsável pelo Risco;

**IX** - pelo chefe da Unidade de Segurança da Informação.

**Art. 10.** Compete ao Comitê de Governança de Segurança da Informação (CGSI):

**I** - assessorar a Alta Administração do Tribunal em questões relacionadas à Segurança da Informação;

**II** - propor alterações e melhorias a esta Política de Segurança da Informação;

**III** - propor normas e procedimentos relativos à Segurança da Informação, visando à operacionalização desta Política;

**IV** - propor atividades de priorização de ações e gestão de riscos de segurança;

**V** - propor recursos necessários à implementação das ações de Segurança da Informação;

**VI** - constituir grupos de trabalho multidisciplinares para tratar normas, procedimentos e temas sobre Segurança da Informação;

**VII** - propor ações visando a fiscalização da aplicação da Política de Segurança da Informação e demais instrumentos;

**VIII** - propor à autoridade competente a abertura de sindicância para investigar e avaliar os danos decorrentes de violação de Segurança da Informação.

**Art. 11.** Deve ser instituído, por ato do Presidente do Tribunal de Justiça do Paraná, uma Unidade de Segurança da Informação, subordinada à Alta Administração do Tribunal.

**§ 1º** A Unidade de Segurança da Informação poderá ser implementada por meio de Comissão Permanente.

**§ 2º** O titular ou responsável pela Unidade de Segurança da Informação será reconhecido como Gestor de Segurança da Informação.

**§ 3º** O Gestor de Segurança da Informação deverá ser Magistrado ou servidor efetivo que possua amplo conhecimento dos processos de negócios do Tribunal e que contenha expertise sobre o tema de Segurança da Informação.

**§ 4º** A Unidade de Segurança da Informação deve ser composta por membros indicados pela Alta Administração, membros do Departamento de Tecnologia da Informação e Comunicação e demais Departamentos pertinentes.

**Art. 12.** Compete à Unidade de Segurança da Informação, instituída no artigo anterior:

**I** - instituir e gerir o Sistema de Gestão de Segurança da Informação (SGSI);

**II** - propor normas relativas à Segurança da Informação ao Comitê de Governança de Segurança da Informação (CGSI);

**III** - propor novas tecnologias na área de Segurança da Informação em conformidade com esta Política;

**IV** - implantar, em conjunto com as demais áreas do Tribunal, normas, procedimentos, planos ou processos elaborados pelo Comitê de Governança de Segurança da Informação (CGSI);

**V** - promover a divulgação desta Política de Segurança da Informação, de outros normativos e de ações para disseminar a cultura em Segurança da Informação no âmbito do Tribunal Justiça do Paraná;

**VI** - definir e acompanhar indicadores de aderência à Política de Segurança da Informação;

**VII** - analisar o andamento dos processos de Segurança da Informação e apresentar suas considerações ao Comitê de Governança de Segurança da Informação (CGSI).

**Art. 13.** Deve ser instituída a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR, contemplando a responsabilidade de receber, analisar, classificar, tratar e responder de forma rápidas, efetivas e ordenadas as notificações e atividades relacionadas a incidentes de segurança em redes de computadores do Tribunal de Justiça do Paraná, além de armazenar registros dos incidentes para fins de estatística e auditoria.

**§ 1º** O modelo de funcionamento e composição de membros do ETIR será proposto pelo Departamento de Tecnologia da Informação e Comunicação - DTIC e aprovado pelo Comitê de Governança de Segurança da Informação.

**§ 2º** A Equipe de Tratamento e Respostas a Incidentes de Segurança Cibernética - ETIR prestará apoio técnico ao CGSI, em temas relacionados aos incidentes de segurança cibernética.

**§ 3º** Excepcionalmente, diante de grave incidente que apresente alto risco à Segurança da Informação, a ETIR terá autonomia para determinar a realização

de procedimentos emergenciais para a sua contenção e recuperação.

§ 4º O processo de gestão de incidentes utilizado pela ETIR será definido em normativo próprio.

**Art. 14.** Compete às unidades administrativas deste Tribunal:

I - apoiar a implementação desta PSI dentro de suas competências;

II - apoiar e buscar os meios para implementar as ações propostas pelo Gestor de Segurança da Informação na execução desta Política;

III - executar as orientações e os procedimentos estabelecidos pelo Comitê de Governança de Segurança da Informação.

**Art. 15.** Compete ao Departamento de Tecnologia da Informação e Comunicação - DTIC:

I - apoiar a implementação desta PSI dentro de suas competências;

II - prover os ativos de processamento de TIC necessários ao cumprimento desta Política de Segurança da Informação;

III - disponibilizar e gerenciar a infraestrutura de TIC necessária aos processos de trabalho para implementação da PSI;

IV - apoiar e buscar os meios para implementar as ações propostas pelo Gestor de Segurança da Informação na execução desta Política;

V - executar as orientações e os procedimentos estabelecidos pelo Comitê de Governança de Segurança da Informação.

## **CAPÍTULO VI**

### **DO PROCESSO DE TRATAMENTO DA INFORMAÇÃO**

**Art. 16.** As políticas, os processos, as práticas e os instrumentos utilizados pelo Poder Judiciário do Estado do Paraná devem abranger o tratamento das informações produzidas ou custodiadas durante o seu ciclo de vida, contemplando o conjunto de ações referentes às fases de produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

**Art. 17.** As informações produzidas ou custodiadas devem ser classificadas e protegidas de acordo com o grau de sigilo e sensibilidade, criticidade, garantindo a sua integridade, disponibilidade e autenticidade.

**§ 1º** Os critérios aplicáveis à classificação e ao tratamento da informação serão definidos por ato normativo da Presidência com a participação de representantes de todas as unidades do Tribunal de Justiça do Paraná.

**§ 2º** Devem ser estabelecidos e utilizados controles criptográficos para o tratamento da informação, em conformidade com todas as leis, acordos, legislação e regulamentações pertinentes, desde que haja recursos técnicos viáveis e disponíveis.

## **CAPÍTULO VII**

### **DAS DISPOSIÇÕES FINAIS**

**Art. 18.** O descumprimento aos dispositivos da Política de Segurança da Informação sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

**Art. 19.** Os contratos, convênios, acordos de cooperação e outros instrumentos semelhantes elaborados pelo Tribunal deverão observar e se adequar a esta Política de Segurança da Informação e seus instrumentos.

**Art. 20.** A Política de Segurança da Informação e a Política de Privacidade e Proteção de Dados Pessoais do TJPR são complementares, devendo ser interpretadas em conjunto.

**Art. 21.** A Política de Segurança da Informação deve ser revisada e atualizada periodicamente, no máximo, a cada 2 (dois) anos.

**Art. 22.** Este Decreto Judiciário entra em vigor na data de sua publicação.

**Art. 23.** Fica revogado o Decreto Judiciário nº 631/2016, de 23 de junho de 2016.

Curitiba, 10 de outubro de 2022.

**Des. JOSÉ LAURINDO DE SOUZA NETTO**

Presidente do Tribunal de Justiça



Documento assinado eletronicamente por **José Laurindo de Souza Netto, Presidente do Tribunal de Justiça**, em 10/10/2022, às 21:10, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site <https://sei.tjpr.jus.br/validar> informando o código verificador **8246507** e o código CRC **6B59370F**.

---

0096656-74.2022.8.16.6000

8246507v4