TEXTO INTEGRAL

RESOLUÇÃO 28/2022

RESOLUÇÃO OE nº 28/2022*

Institui a Estratégia de Segurança da Informação do Poder Judiciário do Estado do Rio de Janeiro.

O ÓRGÃO ESPECIAL DO TRIBUNAL DE JUSTIÇA, no uso de suas atribuições legis, conferidas pelo disposto no inciso XXIII, do art. 17, da Lei de Organização e Divisão Judiciária do Estado do Rio de Janeiro (LODJ), e tendo em vista o decidido na sessão administrativa realizada no dia 03 de outubro de 2022 (Processo SEI n.º 2022-06105729);

CONSIDERANDO os macrodesafios do Poder Judiciário do Estado do Rio de Janeiro para o período 2021--2026, em especial o que trata da "Segurança da Informação e Proteção de Dados";

CONSIDERANDO a Resolução n.º 325 de 28 de janeiro de 2021, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional do Poder Judiciário, para o período 2021-2026;

CONSIDERANDO a Resolução n.º 396 de 7 de junho de 2021, do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a necessidade de assegurar a convergência dos recursos humanos, administrativos e financeiros empregados pelos segmentos do Poder Judiciário no que concerne à Segurança da Informação e Proteção de Dados;

CONSIDERANDO a necessidade de integração das ações no campo da segurança cibernética e da informação, visando proteção das informações e dados do Poder Judiciário do Estado do Rio de Janeiro;

CONSIDERANDO a Resolução TJ/OE n.º 12/2021, que aprovou o Planejamento Estratégico Institucional do Poder Judiciário do Estado do Rio de Janeiro para o biênio 2021/2022;

CONSIDERANDO os estudos realizados no âmbito da Diretoria Geral de Tecnologia da Informação e Comunicação de Dados (DGTEC) sobre segurança da informação de proteção de dados;

CONSIDERANDO a importância de se estabelecer objetivos, princípios e diretrizes de governança de segurança da informação alinhados às recomendações constantes da norma NBR ISO/IEC 27001:2013, que trata do sistema de gestão de segurança da informação, norma NBR ISO/IEC 27014:2021, que trata da governança de segurança da informação e da norma NBR ISO/IEC 27701:2019, que trata da proteção de dados;

CONSIDERANDO ainda que devem ser observadas às boas práticas do Control Objectives for Informationand Related Technology (Cobit 2019) e do Information Technology Infrastructure Library (ITIL 4) de outros modelos de governança e gestão de segurança da informação reconhecidos internacionalmente;

RESOLVE:

Art. 1º. Fica instituída a Estratégia de Segurança da Informação e Cibernética do Poder Judiciário do Estado do Rio de Janeiro (ESIC PJERJ), alinhada a Estratégia Nacional de Segurança da Informação do Poder Judiciário (ENSEC-PJ) e demais diretrizes do Conselho Nacional de Justiça (CNJ).

Art. 2º. Integram a ESIC-PJERJ:

I. a Política de Segurança da Informação (PSI) criada pela Resolução TJ/OE n.º 05 de 25 de fevereiro de 2019;
II. o Protocolo de Prevenção de Incidentes Cibernéticos do PJERJ (PPINC-PJERJ);
III. o Protocolo de Gerenciamento de Crises Cibernéticas do PJERJ (PGCRC-PJERJ);
IV. o Protocolo de Investigação para Ilícitos Cibernéticos do PJERJ (PIILC-PJERJ).

Parágrafo único. As normas técnicas previstas neste artigo devem ser revisadas sempre que necessário, por ato do Presidente do PJERJ.

CAPÍTULO I

DA ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

Art. 3º. A ESIC-PJERJ tem por premissa aprimorar o nível de maturidade em segurança cibernética no Poder Judiciário do Estado do Rio de Janeiro (PJERJ), abrangendo os aspectos fundamentais da segurança da informação para o aperfeiçoamento necessário à consecução desse propósito e com o escopo de tornar as informações e o espaço cibernético mais confiável, resistente, inclusivo e seguro.

Art. 4º. A ESIC-PJERJ contempla os seguintes temas:

I. relacionados à segurança da informação, de forma ampla, que sejam essenciais para segurança cibernética;
II. segurança física e proteção de dados pessoais e institucionais, nos aspectos relacionados à segurança cibernética;
III. segurança física e proteção de ativos de tecnologia da informação de forma geral;
IV. ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e de informações;
V. ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade das atividades fim e administrativas do PJERJ;
VI. ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética;
VII. ações de comunicação, de conscientização, de formação de cultura e de direcionamento institucional com vistas à segurança cibernética; e
VIII. ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de tecnologia da informação e comunicação que atuam na área de segurança cibernética.

Art. 5º. A ESIC-PJERJ está baseada em 3 níveis:

I. numa governança de segurança da informação exercida pela Alta Administração, alinhada com o Planejamento Estratégico Institucional (PEI) do PJERJ;
II. numa gestão de segurança da informação executada pela área de segurança da informação em conjunto com a área de tecnologia da informação e comunicação de dados;
III. numa supervisão das operações de segurança da informação executadas pela área de tecnologia da informação e comunicação de dados.

Art. 6º. São objetivos da ESIC-PJERJ:

I. tornar o PJERJ mais seguro e inclusivo no ambiente digital;
II. aumentar a resiliência às ameaças cibernéticas;
III. estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética no PJERJ; e
IV. permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

CAPÍTULO II
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PJERJ

Art. 7º. São princípios da PSI:

I. segurança jurídica;
II. respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção de privacidade e o acesso à informação;
III. visão abrangente e sistêmica da segurança da informação;
IV. integração, cooperação e intercâmbio científico e tecnológico relacionado à segurança cibernética entre os órgãos estaduais, federais e do meio acadêmico;
V. educação e inovação como alicerce fundamental para o fomento da cultura em segurança da informação;
VI. orientação à gestão de riscos e à gestão da segurança da informação;
VII. prevenção, tratamento e resposta a incidentes cibernéticos;
VIII. articulação entre as ações de segurança cibernética e de proteção de dados e ativos de informação; e
IX. garantia ao sigilo das informações imprescindíveis à segurança da sociedade e do Estado e inviolabilidade da vida privada, da honra e da imagem das pessoas.

Art. 8º. São objetivos da PSI:

I. contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio de ações de segurança da informação, observados os direitos e as garantias fundamentais;
II. fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;
III. aprimorar continuamente o arcabouço normativo relacionado à segurança da informação;
IV. fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação;
V. fortalecer a cultura de segurança da informação no âmbito do PJERJ;
VI. aprimorar o nível de maturidade em segurança da informação do PJERJ;
VII. orientar ações relacionadas:
a) à gestão em segurança da informação;
b). à segurança da informação das infraestruturas críticas;
c) ao tratamento das informações com restrições de acesso;
d) à proteção dos dados pessoais e dos dados pessoais sensíveis, em conformidade com legislação específica;
e) à prevenção, ao tratamento e à resposta a incidentes cibernéticos;
f) à gestão e operação de equipe de tratamento e resposta a incidentes cibernéticos;
g) ao estabelecimento dos níveis de maturidade em segurança da informação; e
h) ao estabelecimento de processo transparente de comunicação e respostas a incidentes entre o poder público e a sociedade.

Art. 9º. A PSI deverá estabelecer ainda ações para:

I. realizar a Gestão dos Ativos de Informação e da Política de Controle de Acesso;
II. criar controles para o tratamento de informações com restrição de acesso;
III. promover treinamento contínuo e certificação internacional dos profissionais diretamente envolvidos na área de segurança cibernética;
IV. estabelecer requisitos mínimos de segurança da informação nas contratações e nos acordos que envolvam a comunicação com outros órgãos;
V. utilizar os recursos de soluções de criptografia, ampliando o uso de assinatura eletrônica, conforme legislações específicas; e
VI. comunicar e articular as ações de segurança da informação com a alta administração do órgão.

Art. 10. A PSI deve estabelecer regras para o tratamento de dados pessoais de acordo com a Lei n.º 13.709/2018 (LGPD).

Art. 11. As normas gerais e específicas de governança e gestão de SI, emanadas no âmbito do PJERJ, são consideradas também parte integrante da PSI a que se refere esta Resolução.

CAPÍTULO III
DA ESTRUTURA DE GOVERNANÇA E GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Seção I
Do Comitê de Governança de Segurança da Informação (CGSI)

Art. 12. A governança de Segurança da Informação do PJERJ será coordenada pelo Comitê de Governança de Segurança da Informação do PJERJ (CGSI), de acordo com as diretrizes estabelecidas pelo CNJ, com o objetivo de elaborar e aplicar política, gestão e processo de segurança da informação e comunicação a serem desenvolvidos em todos os níveis da instituição e em harmonia com as diretrizes nacionais preconizadas pelo CNJ e das normas internacionais de segurança da informação baseadas em Confidencialidade, Integridade, Disponibilidade e Autenticidade.

§ 1º. O CGSI é órgão colegiado de natureza deliberativa e de caráter permanente, com responsabilidades de cunho estratégico e executivo, dentro de sua área de atuação.

§ 2º. O CGSI deverá contar com estrutura mínima compatível com suas atribuições.

Art. 13. O CGSI será composto pelos seguintes membros da Alta Administração:

I. um Desembargador, que o presidirá, indicado pelo Presidente do PJERJ;
II. o Desembargador Presidente da COSEG;
III. o Desembargador Presidente do CGPDP;
IV. o Desembargador Presidente do CGTIC;

V. um Juiz Auxiliar da Presidência do PJERJ que será o seu coordenador;
VI. dois Juízes de Direito, indicados pelo Presidente do PJERJ;
VII. um Juiz Auxiliar da Corregedoria Geral da Justiça;
VIII. um Juiz de Direito indicado pela AMAERJ;

Parágrafo único. Para o desempenho de suas funções, o CGSI contará com um representante do órgão responsável pelo apoio aos Órgãos Colegiados Administrativos para secretariá lo.

Art. 14. O CGSI contará com a participação de:

I. os seguintes Diretores:

a) o Diretor Geral de Tecnologia da Informação e Comunicação de Dados;
b) o Diretor Geral de Segurança Institucional;
c) o Diretor Geral de Comunicação e de Difusão do Conhecimento;
d) o Diretor de Segurança da Informação;

II. membros da área técnica, sendo no mínimo:

a) um representante da Diretoria de Segurança da Informação com especialidade em gestão Segurança da Informação;
b) um represente da DGTEC com especialidade em operação de Segurança da Informação;
c) um representante da DGSEI com especialidade em telecomunicações;
d) um representante da DGSEI com especialidade em segurança física;
e) um representante da DGCOM com especialidade em comunicações.

III. membros da área institucional e jurisdicional:
a) um represente da DGJUR;
b) um representante da área de gestão estratégica e planejamento;
c) um representante da CGJ.

§ 1º. Os membros CGSI serão nomeados por meio de Ato do Presidente do PJERJ.
§ 2º. As deliberações do CGSI são tomadas por maioria, com voto de qualidade do seu Presidente em caso de empate.
§ 3º. O Presidente do CGSI indicará um dos servidores como Secretário-Executivo, para a coordenação administrativa.
§ 4º. Caberá ao CGSI atuar como Comitê de Crises Cibernéticas em todas as ocasiões em que se caracterizar uma crise cibernética, conforme os requisitos estabelecidos no Protocolo de Gerenciamento de Crises Cibernéticas do PJERJ.
§ 5º. Caberá a Divisão de Apoio e Assessoramento Técnico aos Órgãos Colegiados Administrativos (DEGEP/DICOL) o apoio administrativo ao CGSI.

Art. 15. Compete ao CGSI, dentre outras atribuições deferidas pelo Presidente do PJERJ:

I. avaliar, do ponto de vista da segurança da informação e comunicação, os sistemas de informação do PJERJ, aprovando se as atualizações, revisões e desativações atendem os requisitos de segurança;
II. recomendar padrões e procedimentos técnicos de segurança a serem utilizados na área de TIC e de segurança da informação, especialmente em relação ao uso da Internet e da Intranet;
III. recomendar adoção de metodologias de desenvolvimento de sistemas e inventário dos principais sistemas e base de dados, que atendam as boas práticas de segurança da informação e comunicação;
IV. estabelecer as políticas de segurança da informação e comunicação na área de TIC;
V. estabelecer política de minimização dos riscos e do aumento no nível de segurança das informações do PJERJ, compreendendo, no mínimo, a disponibilidade, a integridade, a confiabilidade, a autenticidade e o sigilo das informações;
VI. coordenar a revisão periódica de normas do PJERJ que visem aperfeiçoar a segurança da informação, para aprovação do Presidente do PJERJ;
VII. estabelecer mecanismos de coleta, organização e disseminação de informações de forma segura, sobre os serviços Internet/Intranet, bem como dos novos sistemas e tecnologias existentes no mercado;
VIII. participar de fórum de debates com instituições que desenvolvam projetos de pesquisa ou estudos sobre segurança da informação, bem como, ser órgão difusor dessas participações junto às demais unidades do PJERJ;
IX. encaminhar anualmente a Alta Administração as propostas de melhorias e ajustes julgados necessários, informações consolidadas sobre a situação da segurança da informação no PJERJ;
X. promover a adequada publicidade e transparência das informações relativas à segurança da informação;

XI. diligenciar junto a área de segurança da informação a implementação da política de minimização dos riscos e do aumento no nível de segurança das informações do PJERJ definida pelo CGSI;
XII. supervisionar os indicadores de desempenho relacionados à segurança da informação;
XIII. atuar como órgão técnico em matéria de segurança da informação junto ao Presidente do PJERJ em assuntos não regulamentados ou omissos;
XIV. propor a aplicação de ações corretivas e disciplinares cabíveis nos casos de violação de segurança da informação.
XV. garantir a implementação de todas a diretrizes, protocolos e manuais estabelecidos pelo CNJ para área de segurança da informação;
XVI. estabelecer uma política de aculturamento e treinamento na área de segurança da informação;
XVII. encaminhar anualmente, até o mês de abril, ao Presidente do PJERJ proposta orçamentária para área de segurança da informação;
XVIII. aprovar anualmente até o mês de junho o plano de capacitação dos profissionais da área de segurança da informação para o exercício seguinte;
XIX. coordenar o Gabinete de Crise em caso de incidentes de segurança da informação.

§ 1º. Caberá ao CGSI desenvolver ações estruturantes e de controle para a plena implantação do alinhamento estratégico e para o estabelecimento de metas anuais, em conformidade com os Objetivos Estratégicos do PJERJ, ou, ainda, para o cumprimento dos compromissos periódicos acerca das demandas de segurança da Informação.
§ 2º. Para desenvolvimento das atividades e cumprimento de suas atribuições o CGSI poderá constituir comissões temáticas ou grupos de trabalho, assim como solicitar apoio e auxílio técnico de outras unidades e servidores do PJERJ.
§ 3º. Os membros das comissões ou grupos de trabalho serão indicados pelo Presidente do CGSI e nomeados por ato do Presidente do PJERJ.
§ 4º. As comissões ou grupos de trabalho deverão submeter à apreciação do CGSI pareceres sobre as solicitações ou alterações propostas para avaliação e aprovação.

Art. 16. Caberá ao CGSI propor, ao Presidente do PJERJ, com o suporte técnico da do Departamento de Segurança da Informação e do ETIR, ato normativo estabelecendo regras de gestão de riscos de SI e continuidade de serviços essenciais.

Seção II
Da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR)

Art. 17. Fica instituída, no âmbito do PJERJ, a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR), vinculado ao Comitê de Governança de Segurança da Informação do Tribunal de Justiça do Estado do Rio de Janeiro (CGSI), conforme estabelece a Resolução CNJ n.º 396, de 7 de junho de 2021.

Parágrafo único. A ETIR é um órgão colegiado que atuará tecnicamente em todos os incidentes de segurança da informação, fornecendo suporte ao CGSI, sempre que demandado.

Art. 18. A ETIR será composta da seguinte forma:

I. o Diretor Segurança da informação, que a presidirá;
II. o Diretor Geral de Tecnologia da Informação e Comunicação de Dados;
III. 3 (três) especialistas em gestão de segurança da informação do Departamento de Segurança da Informação;
IV. 2 (dois) especialistas em operações de segurança da informação da DGTEC;
V. 2 (dois) especialistas em segurança institucional e de comunicações da DGSEI;

§ 1º. Os membros da ETIR serão nomeados por meio de Ato do Presidente do PJERJ.
§ 2º. A ETIR deverá dar ciência de suas decisões operacionais e táticas, sempre que possível com antecedência e submeter as propostas estratégicas ao CGSI.

Art. 19. Compete a ETIR, no âmbito do PJERJ, dentre outras atribuições deferidas pelo CGSI:

I. propor e implantar procedimento de tratamento e resposta a incidentes em segurança da informação;
II. propor a criação e acompanhar indicadores de desempenho táticos e operacionais que auxiliem o monitoramento dos serviços gerenciados de segurança da informação, visando a sua melhoria contínua;

III. recomendar padrões e procedimentos técnicos operacionais para todos os usuários do PJERJ;
IV. relatar, acompanhar e supervisionar tecnicamente todos os incidentes de segurança da informação e as respectivas soluções de forma adequada.
V. apoiar tecnicamente o CGTIC no planejamento estratégico, projetos e demandas de TIC;
VI. participar obrigatoriamente das reuniões do Gabinete de Crise em caso de incidentes de segurança da informação;
VII. participar da Rede de Cooperação do Judiciário na área de segurança cibernética, através do Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC PJ) criado pelo CNJ;
VIII. apresentar ao CGSI relatório sobre os indicadores de desempenho dos serviços gerenciados de segurança da informação adotados pelo PJERJ;
IX. auxiliar o CGSI em tudo que for necessário para o desempenho de suas atribuições.

Parágrafo único. Os dois membros da ETIR que participação da Rede de Cooperação do Judiciário na área de segurança da informação serão nomeados por meio de Ato do Presidente do PJERJ e indicados ao CNJ.

Seção III
Do Departamento de Segurança da Informação

Art. 20. Compete ao Departamento de Segurança da Informação, para efeito do disposto nesta Resolução, dentre outras atribuições determinadas pelo CGSI e em atos normativos do PJERJ:

I. ser o responsável pela implantação e gerenciamento de um Sistema de Gestão de Segurança da Informação
II. executar o planejamento estabelecido no PDTIC, na parte de Segurança da Informação (SI);
III. propor ao CGSI a definição de processos de trabalho, métodos, técnicas, ferramentas, arquitetura e padrões aplicáveis ao provimento de soluções de segurança da informação, em conformidade com os princípios e diretrizes estabelecidos nesta Resolução, diretrizes do CNJ e frameworks de mercado;
IV. realizar o provimento centralizado e descentralizado de soluções de SI e assegurar seu funcionamento em conformidade com os níveis de serviço acordados com as unidades gestoras de soluções;
V. submeter ao CGSI as demandas relativas ao provimento centralizado e descentralizado de novas soluções de SI;
VI. encaminhar ao CGSI todos os processos de sua competência devida instruídos para deliberação;
VII. apoiar o CGSI no planejamento e na execução de ações de desenvolvimento de competências relativas ao provimento, à governança, à gestão de SI;
VIII. propor ao CGSI a alocação de recursos orçamentários destinados à SI;
IX. trabalhar de forma integrada com o ETIR do PJERJ;
X. apresentar ao CGSI relatório do uso de recursos para contratação da área de SI;
XI. estabelecer ações que visem a adequação das bases de dados do PJERJ a proteção de dados pessoais de acordo com a Lei n.º 13.709/2018 (LGPD);
XII. propor os ajustes necessários a fim de otimizar o uso dos recursos orçamentários destinados à SI;
XIII. propor ao CGSI cursos de capacitação para os profissionais e técnicos da área de SI; e
XIV. auxiliar o CGSI em tudo que for necessário para o desempenho de suas atribuições.

CAPÍTULO IV
DA GOVERNANÇA E DA GESTÃO DE SI

Art. 21. A governança, a gestão de SI no âmbito do PJERJ orientam se, no que couber, pelas boas práticas preconizadas por normas e modelos adotados como referência pelo Tribunal Contas da União, do Estado e do CNJ no exercício do controle externo relativo ao tema, e pelos seguintes objetivos:

I. promover a coordenação dos diversos entes do PJERJ relacionados com a segurança da informação;
II. contribuir para a resiliência corporativa por meio de resposta, tão célere e eficiente quanto possível, a incidentes em que os ativos de informação do PJERJ possam ter a sua confidencialidade, integridade, ou disponibilidade comprometidas;
III. estabelecer e desenvolver padrão de maturidade unificado de segurança da informação, de forma que seja possível avaliar o nível de maturidade em segurança da informação do PJERJ, por meio de indicadores estabelecidos;
IV. estabelecer rotinas de verificações de conformidade em segurança da informação;
V. possibilitar a convergência de esforços e iniciativas na apuração de incidentes e na promoção de ações de capacitação e educação em segurança da informação;
VI. definição formal de autoridade e responsabilidade por decisões e ações;
VII. alinhamento dos planos e ações de SI às estratégias de negócio, ao planejamento estratégico, ao plano plurianual e às necessidades do PJERJ;
VIII. otimização dos processos de trabalho e do uso de recursos do PJERJ;
IX. formalização de diretrizes, processos de trabalho e procedimentos;

X. identificação e gestão de riscos organizacionais, de tecnologia e de ambiente;
XI. produção, disseminação e preservação de conhecimentos referentes a processos de trabalho e regras de negócio associados a soluções de SI;
XII. conformidade com disposições legais e atos administrativos do CNJ e do PJERJ; e
XIII. monitoração e avaliação regular, pela alta Administração, do alcance das metas definidas nos planos de SI e da conformidade e desempenho dos processos que suportam a política de SI do PJERJ.

Art. 22. A Gestão de SI deve contemplar ainda:

I. a gestão de incidentes e problemas de SI;
II. a gestão de ativos de SI;
III. a gestão de usuários;
IV. a gestão de riscos de SI;
V. a gestão de continuidade de serviços;
VI. a política educacional e cultural em segurança da informação; e
VII. a gestão de orçamento de SI.

Parágrafo único. Toda a gestão de SI será disciplinada por atos do Presidente do PJERJ.

Art. 23. A gestão de incidentes deve estabelecer regras para o monitoramento e o tratamento de incidentes de SI, bem como a investigação de problemas no âmbito do PJERJ.

Art. 24. A gestão de ativos deverá estabelecer quais são os ativos de SI do PJERJ e como deverão ser gerenciados, incluindo desenvolvimento seguro e serviços em nuvem.

Art. 25. A gestão de usuários de sistemas informatizados composta, no mínimo, de:

I. gerenciamento de identidades;
II. gerenciamento de acessos; e
III. gerenciamento de privilégios.

Art. 26. A gestão de riscos de SI deve estabelecer, no mínimo, regras para levantamento de riscos de SI, criação de matriz e tratamento de riscos de SI.

Art. 27. A gestão de continuidade de serviços deve prever, no mínimo, os serviços essenciais, manutenção e recuperação dos serviços.

Art. 28. A política educacional e cultural deve estabelecer regras para criação de uma cultura em segurança da informação em todo o PJERJ com atividades constantes segmentando o público interno e externo, além de capacitação especializada para área técnica.

Art. 29. A gestão de orçamento de SI deve contemplar recursos necessários para execução das ações estratégicas da área de SI, discriminados em rubrica específica em consonância com as diretrizes do CNJ.

Art. 30. O PJERJ deverá manter quadro de pessoal permanente de profissionais da área de SI, compatível com a demanda e o seu porte, de forma a atender os requisitos estabelecidos na Resolução CNJ n.º 396/2021.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 31. O Departamento de Segurança da Informação deverá providenciar em 180 (cento e oitenta) dias a contar da publicação da presente Resolução a revisão técnica de documentos e normas vigentes no PJERJ, referentes a área de SI, no que couber, nos termos previstos nesta Resolução encaminhar ao CGSI para deliberação.

Art. 32. Os casos omissos na aplicação dos dispositivos desta Resolução serão resolvidos pelo CGSI dentro de suas atribuições.

Art. 33. A presente Resolução entrará em vigor na data de sua publicação, revogando as disposições em contrário.

Rio de Janeiro, 03 de outubro de 2022.

Desembargador HENRIQUE CARLOS DE ANDRADE FIGUEIRA
Presidente

*Republicada por incorreção material no DJERJ do dia 04/10/2022.