PODER JUDICIÁRIO DO ESTADO DO PIAUÍ
COORDENADORIA ADMINISTRATIVA DO PLENO - PLENOADM
Pça Des. Edgard Nogueira s/n - Bairro Cabral - Centro Cívico - CEP 64000-830
Teresina - PI - www.tjpi.jus.br

Resolução Nº 39/2021 - PJPI/TJPI/SECPRE/PLENOADM

RESOLUÇÃO Nº 232/2021, DE 05 DE JULHO DE 2021

Dispõe, no âmbito do Tribunal de Justiça do Estado do Piauí - TJPI, sobre o Sistema de Gestão de Segurança da Informação - SGSI e a Política de Segurança da Informação – PSI

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO PIAUÍ, no uso de suas legais e regimentais, e considerando a deliberação plenária ocorrida na 93ª sessão ordinária administrativa realizada em 05 de julho de 2021,

CONSIDERANDO a Lei 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI);

CONSIDERANDO as normas ABNT NBR ISO/IEC 27001:2013, 27002:2013, 27003:2011, 27004:2010, 27005:2011, 22301:2019, 27014:2013;

CONSIDERANDO, ainda, a Resolução nº 396, de 7 de junho de 2021, que Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), e Portaria nº 162, de 10 de junho de 2021;

RESOLVE:

TÍTULO I
DISPOSIÇÕES GERAIS

CAPÍTULO I
DO OBJETIVO

Art. 1º O objetivo desta Resolução é estabelecer, implementar, manter e melhorar, continuamente, mecanismos e controles para promover a gestão da segurança da informação, de forma a garantir o direito de acesso previsto em Lei, a proteção dedados, informações e conhecimentos gerados e custodiados, a redução de riscos de ocorrência de perdas, alterações e acessos indevidos, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações, no âmbito do Tribunal de Justiça do Estado do Piauí - TJPI.

CAPÍTULO II
DA ABRANGÊNCIA

Art. 2º As normas desta Resolução aplicam-se a todas as autoridades, servidores, colaboradores e quaisquer pessoas que tenham acesso a informações do TJPI.

Parágrafo único. A segurança da informação abrange aspectos físicos, tecnológicos e humanos do TJPI.

CAPÍTULO III
DOS PRINCÍPIOS

Art. 3º A segurança da informação no TJPI alinha-se às estratégias organizacionais e aos seguintes princípios:

I - a preservação da disponibilidade, integridade, confiabilidade e autenticidade dos dados, informações e conhecimentos que compõem o ativo da informação do TJPI;

II - continuidade das atividades;

III - economicidade da proteção dos ativos de informação;

IV - pessoalidade e utilidade do acesso aos ativos de informação;

V - a responsabilização do usuário pelos atos que comprometam a segurança dos ativos de informação;

VI - observância da publicidade como preceito geral e do sigilo como exceção;

VII - divulgação de informações de interesse público, independentemente de solicitações;

VIII - utilização de meios de comunicação viabilizados pela tecnologia da informação;

IX - fomento ao desenvolvimento da cultura da transparência na Administração Pública;

X - contribuição para o desenvolvimento do controle social da Administração Pública.

CAPÍTULO IV
DOS CONCEITOS

Art. 4º Para os efeitos desta Resolução, entende-se por:

I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato, incluindo peças processuais;

II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;

III - segurança da informação: tratamento da informação de forma a garantir sua disponibilidade, integridade, autenticidade, confiabilidade, primariedade e confidencialidade, quando necessário, bem como minimizar riscos, promover a eficácia das ações do negócio e preservar a imagem do TJPI;

IV - Sistema de Gestão de Segurança da Informação - SGSI: conjunto de mecanismos inter-relacionados, baseado em riscos do negócio, que visa estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação;

V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;

VI - disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos recursos correspondentes sempre que necessário;

VII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;

VIII - autenticidade: consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações.

IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações;

X - confidencialidade: propriedade que garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para tal;

XI - incidente de segurança da informação: qualquer indício de fraude, sabotagem, espionagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer ou ameaçar a segurança da informação;

XII - gestor da informação: colegiado, autoridade ou gestor de unidade responsável por informação em matéria de sua competência ou inerente a sua área de atuação;

XIII - custodiante da informação: qualquer pessoa física ou jurídica, interna ou externa, unidade ou projeto do Tribunal que detém a posse, mesmo que transitória, de informação produzida ou recebida pelo Tribunal;

XIV - ciclo de vida da informação: compreende etapas e eventos de produção, recebimento, armazenamento, acesso, uso, alteração, cópia, transporte e descarte da informação;

XV - colaborador: prestador de serviço terceirizado, estagiário ou qualquer pessoa com vínculo transitório com o TJPI que tenha acesso, de forma autorizada, às informações ou às dependências do Tribunal;

XVI - informação não pública: informação com restrições de acesso previstas em instrumentos normativos;

XVII - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado;

XVIII - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável;

XIV - ameaça: qualquer circunstância ou evento com o potencial de causar dano ou violação sobre a confidencialidade, a integridade, a autenticidade e a disponibilidade da informação, do sistema ou da organização;

XV - Comitê Gestor de Segurança da Informação - CGSI: comitê composto por representantes de áreas relevantes do TJPI, responsável pela formulação, implementação, acompanhamento e revisão das ações de segurança pertinentes;

XVI - continuidade de serviços essenciais de TIC: capacidade estratégica e tática do TJPI de se planejar e responder a incidentes e interrupções devido às vulnerabilidades de TIC, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;

TÍTULO II

DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO - SGSI

Art. 5º O Sistema de Gestão de Segurança da Informação - SGSI é composto pelos seguintes processos e protocolos:

I - classificação da informação;

II - gestão de riscos de segurança da informação;

III - gestão de incidentes em segurança da informação;

IV - gestão da garantia e controle de acesso à informação;

V - segurança da informação em recursos humanos e conscientização em segurança da informação;

VI - serviço de correio institucional;

VII - backup e recuperação de dados;

VIII - segurança em tecnologia da informação e comunicações;

IX - Protocolo de Prevenção a Incidentes Cibernéticos no âmbito do Poder Judiciário (PPICiber/PJ);

X - Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PGCC/PJ);

XI - Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário;

§ 1º Os processos do SGSI, a serem regulamentados em políticas específicas, são interdependentes e devem ser estruturados e monitorados de forma a permitir sua melhoria contínua a serem apresentados a gestão superior.

§ 2º A Gestão de Continuidade de Negócios - GCN, disposta em política específica, harmoniza-se com os processos do SGSI e tem por objetivo, em relação à segurança da informação, garantir níveis adequados de disponibilidade, integridade, confiabilidade, primariedade, autenticidade e confidencialidade, quando necessário, das informações essenciais ao funcionamento dos processos críticos de negócio do TJPI. Em relação a Gestão de Continuidade de Negócios de TIC a política deve ser apresentada a gestão superior.

Art. 6º Fica criada a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI, subordinada à Secretaria de Tecnologia da Informação e Comunicações e coordenada pelo Coordenador de Infraestrutura e pelo Chefe de Seção de Segurança da Informação.

I - As atribuições da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETRI são regulados no anexo específico desta Portaria.

II - A ETRI é composta por servidores da Secretaria de Tecnologia da Informação e Comunicações, sendo:

a) o Coordenador de Infraestrutura de TIC;

b) o Coordenador de Software;

c) o Coordenador de Governança de TI;

d) o Chefe de Seção de Segurança da Informação;

e) o Chefe de Seção de Suporte e Manutenção;

f) o Chefe de Seção de Redes de Comunicação;

g) o Chefe de Seção de Banco de Dados;

CAPÍTULO I
DAS DIRETRIZES

Seção I
Da conscientização e da capacitação

Art. 7º As diretrizes básicas da Política de Segurança da Informação - PSI devem ser divulgadas em todas as unidades do TJPI, garantindo que todos tenham consciência da Política e a pratiquem.

Art. 8º Os usuários, por ocasião do início de suas atividades no Poder Judiciário do Estado do Piauí, deverão formalizar a ciência do conteúdo desta política e de suas normas

complementares, mediante assinatura da Declaração de Aceitação junto ao seu processo de admissão no TJPI.

Art. 9º Por ocasião da exoneração ou aposentadoria de servidor, magistrado ou colaborador ou por término de vigência contratual de terceirizados, mirins e estagiários, deverá ser observado um processo de descredenciamento de acesso no ato do desligamento.

Art. 10. Os servidores e colaboradores devem ser continuamente capacitados para o uso dos ativos de informação por ocasião da realização de suas atividades.

Art. 11. Programas de conscientização sobre segurança da informação serão implementados através de treinamentos específicos, assegurando que todos os servidores e colaboradores sejam informados sobre a exigência de garantir acesso à informação como regra geral e sobre os potenciais riscos de segurança e o tipo de exposição a que estão submetidas as informações de caráter sigiloso ou restrito.

Art. 12. Os treinamentos a serem disponibilizados devem estar compatíveis com as tecnologias atualmente implementadas no ambiente informatizado e com as demais que porventura venham a ser adotadas.

I - O Plano de Capacitação de Servidores de TIC deverá contemplar o tema de Segurança da Informação como processo contínuo, com revisão periódica.

II - O Plano de Capacitação de Usuários de TIC deverá contemplar o tema de Política da Segurança da Informação como processo contínuo, com revisão periódica. Cabendo à STIC manter um plano de curso atualizado com a PSI.

Art. 13. As propostas de treinamento e capacitação poderão ser apresentadas por qualquer setor do TJPI e serão dirigidas à Comitê de Segurança da Informação.

Parágrafo único. O Comitê de Segurança da Informação fará uma análise preliminar acerca da conveniência da proposta e, caso entenda oportuna, encaminhará a proposta à Secretaria Geral do TJPI, que tomará as providências perante o Diretor Geral da EJUD.

Seção II

Da garantia e do controle de acesso

Art. 14. A publicidade de informações é preceito geral, e o sigilo é exceção.

§ 1º Qualquer falha na segurança da informação, relacionada à garantia ou ao controle de acesso, identificada por qualquer servidor ou colaborador, deve ser imediatamente comunicada ao seu superior imediato, que a encaminhará à STIC para avaliação e determinações das ações que se fizerem necessárias.

§ 2º O acesso a sistemas de informação do TJPI deve ser controlado de acordo com o valor, sensibilidade e criticidade da informação nele contida e considerando aspectos de restrição legais e/ou normativos.

Art. 15. As informações produzidas por servidores e quaisquer colaboradores do TJPI, no exercício de suas atribuições, são patrimônio intelectual do Tribunal e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento da autoria, se for o caso.

§ 1º Quando as informações forem produzidas por colaboradores do TJPI para uso exclusivo pelo Tribunal, instrumento próprio estabelecerá as obrigações dos criadores, inclusive no que se refere à eventual confidencialidade das informações.

§ 2º É vedada a utilização das informações a que se refere o § 1º deste artigo em projetos ou atividades diversas daquelas estabelecidas pelo TJPI, salvo autorização específica dos desembargadores e juízes, nos processos e documentos de sua competência, Presidente ou Corregedor, conforme os casos.

Art. 16. O processo de controle de acesso à informação tem por objetivo garantir que o acesso físico e lógico à informação seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e de segurança da informação.

§ 1º O acesso às informações não públicas produzidas ou custodiadas pelo TJPI deve permanecer restrito às pessoas que tenham necessidade de conhecê-las.

§ 2º O acesso a informações não públicas por quaisquer colaboradores é condicionado ao aceite de termo de sigilo e responsabilidade.

§ 3º O acesso às informações produzidas ou custodiadas pelo TJPI se submete a controles administrativos e tecnológicos definidos de acordo com a respectiva classificação.

§ 4º Mesmo que as informações, máquinas virtuais, bancos de dados e demais artefatos tecnológicos estejam hospedados em infraestrutura de terceiros, o controle de acesso e as respectivas máquinas ficam submetidos ao controle da Secretaria de Tecnologia da Informação e os colaboradores condicionado ao aceite de termo de sigilo e responsabilidade.

Art. 17. Todos os servidores e colaboradores que manipulem ou tenham acesso a informações identificadas como sigilosas sob custódia ou de propriedade do TJPI devem garantir a confidencialidade e o segredo dessas informações, adotando comportamento seguro, caracterizado por evitar assuntos sigilosos em ambientes sociais e particulares, impressão, transmissão, compartilhamento e transporte para fora das instalações do TJPI de informação sigilosa, sem autorização, bem como uso e não compartilhamento de senhas seguras que deverão ser renovadas anualmente e ter duplo fator de autenticação.

§ 1º A Coordenação de Softwares da STIC providenciará no prazo de 30 (trinta) dias da publicação desta Resolução aplicativo de renovação de senha, bem como o travamento para renovação nos principais sistemas administrativos e judiciais.

§ 2º As senhas atenderão ao nível alto de segurança tendo, no mínimo, 8 (oito) caracteres, atender aos requisitos de incluir números e letras maiúsculas e minúsculas, incluir um caractere especial que não seja letra nem número, expirar após um ano de uso e a nova senha deve ser diferente das últimas 5 (cinco) senhas usadas.

Art. 18. As violações de segurança devem ser comunicadas e registradas, e esses registros, analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

Art. 19. Compete ao Comitê de Segurança de Informação atuar com o objetivo de:

I - fazer cumprir os requisitos legais ou normativos relacionados à garantia de acesso e à qualidade da informação, especialmente quanto à objetividade, transparência, clareza e utilização de linguagem de fácil compreensão.

II - propor às unidades competentes a publicação de informações de interesse geral produzidas ou custodiadas pelo TJPI, independentemente de requerimento.

Seção III

Da segurança física e do ambiente de recursos humanos

Art. 20. A segurança física e patrimonial, disposta em política específica elaborada, tem por objetivo, em relação à segurança da informação, prevenir danos e interferências nas instalações do TJPI que possam causar perda, roubo ou comprometimento das informações.

Parágrafo único. Compete à Superintendência de Segurança planejar, estabelecer, monitorar e revisar periodicamente a Política e procedimentos de segurança física do TJPI em regulamentos específicos que deverão ser apresentados anualmente ao Comitê de Segurança da Informação no prazo de 1 (um) ano da publicação desta Resolução.

Art. 21. Tendo em vista a necessidade de garantir a segurança física e do ambiente, bem como a segurança de recursos humanos, deverão ser estabelecidos controles visando a:

I - prevenir o acesso físico indevido e sem autorização, devendo todo usuário ser identificado antes de adentrar aos prédios do TJPI, visando evitar danos e interferências nas instalações dos ativos de TI e informações do TJPI;

II - assegurar que servidores, colaboradores, fornecedores e terceiros entendam suas responsabilidades e assinem acordos sobre seus papéis e responsabilidades pela segurança da informação, com a finalidade de reduzir os riscos de burla, erros humanos, furto, roubo, apropriação indébita, fraude ou uso indevido dos ativos de TI e de informações do TJPI;

III - as salas e raques que acomodem equipamento de comunicação de dados, devem ser exclusivas para esses equipamentos, com seu controle de acesso gerenciado pela Seção de Redes de Comunicação ou diretor do fórum.

Seção IV

Do plano de continuidade

Art. 22. Os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos, observando-se as classificações de disponibilidades requeridas, de forma a não permitir a interrupção das atividades de negócios e a proteger os processos críticos contra falhas e danos, que atenderão aos seguintes objetivos e estarão sempre em harmonia com as normas do Conselho Nacional de Justiça - CNJ, em relação à Segurança da informação:

I - avaliação em regime emergencial das consequências de desastres, falhas de segurança e perda de serviços;

II - contingência e recuperação do funcionamento normal dentro de períodos de tempos determinados;

III - recuperação tempestiva das operações consideradas vitais.

IV - Os recursos que suportam funções críticas são definidos por normativo próprio que define os sistemas essenciais de TIC, que deverão ser alvo de medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e na estratégia de gestão de riscos.

Art. 23. Fica criado o Comitê Gestor de Segurança da Informação - CGSI, composto por cinco membros:

I – o Desembargador Presidente do Comitê de Governança de Tecnologia da Informação e Comunicações, que o presidirá;

II – um Juiz Auxiliar da Presidência;

III – um Juiz Auxiliar da Corregedoria;

IV – o Secretário-Geral da Presidência;

V – o Secretario de Tecnologia da Informação e Comunicação;

VI - o Coordenador de Infraestrutura de TIC;

VII - o Chefe da Seção de Segurança da Informação.

Art. 24. Compete ao Coordenador de Infraestrutura de TIC e ao Chefe da Seção de Segurança da Informação estabelecerem e revisar periodicamente um plano de continuidade de TIC que será regulado em normativo específico.

Art. 25. O funcionamento do CGSI será regulado em normativo específico e tem por objetivo monitorar e gerenciar, inclusive durante os desastres, o plano de continuidade de TIC, os Protocolos de Prevenção a Incidentes, o Gerenciamento de Crises e o Protocolo de Investigação de ilícitos Cibernéticos.

Seção V

Da conformidade

Art. 26. Devem ser adotados procedimentos apropriados para garantir a conformidade e o respeito às exigências legais quanto à disponibilização de informações públicas, bem como ao uso e disseminação de informações protegidas por leis tais como: dados pessoais relativos à intimidade, à vida privada, à honra e à imagem, de propriedade intelectual, direitos autorais, segredos comerciais e de indústria, patentes e marcas registradas ou aquelas classificadas como sigilosas.

Art. 27. Os processos de aquisição de bens e serviços, especialmente dos ativos de informação, devem estar em conformidade com esta Resolução e com o Regimento Interno Administrativo da Secretaria do TJPI.

Art. 28. Os sistemas de informações, além de disponibilizar os registros em prazos e formatos que atendam as exigências legais, devem protegê-los contra perda, destruição e falsificação, visando à salvaguarda dos dados. Os softwares utilizados pelo Poder Judiciário do Estado do Piauí devem ser previamente licenciados e homologados pela Secretaria de Tecnologia da Informação, que considerará, dentre outros, os aspectos de segurança, aderência à metodologia de desenvolvimento de sistemas e suporte a usuários.

§ 1º O Processo de Desenvolvimento de Software do TJPI deve considerar as boas práticas de desenvolvimento com foco em segurança da informação, de forma a preservar o ambiente tecnológico, assim como prevenir possíveis vulnerabilidades e incidentes que afetem a autenticidade, a confidencialidade, a integridade e a disponibilidade das informações e dos recursos de TIC do TJPI.

§ 2º A Secretaria de Tecnologia de Informação, antes de autorizar a instalação e uso do software, realizará estudos de viabilidade e os testes necessários que atestem sua compatibilidade com o regular desenvolvimento das atividades laborais do Poder Judiciário do Estado do Piauí.

§ 3º Todos os elementos necessários para a plena continuidade do negócio devem ter sua operacionalidade garantida em softwares que por ventura tenham sido desenvolvidos fora das dependências da STIC, ficando, doravante, terminantemente proibido do desenvolvimento de softwares sem a supervisão da STIC/Coordenação de Software, devendo os sistemas que se encontrem nesta situação serem submetidos a planos de migração ou descontinuidade para a administração da STIC no prazo de 6 (seis) meses da publicação desta Resolução.

Seção VI

Da classificação e do sigilo da informação

Art. 29. A classificação da informação tem por objetivo assegurar que a informação receba um nível adequado de proteção.

Parágrafo único. A informação deve ser classificada para indicar a necessidade, as prioridades e o nível esperado de proteção quanto ao tratamento da informação durante todo o seu ciclo de vida.

Art. 30. Compete à Comissão Permanente de Avaliação Documental do TJPI, planejar, estabelecer regulamentos específicos, monitorar e revisar periodicamente a classificação da informação do TJPI.

Art. 31. Toda informação não classificada terá caráter ostensivo e deverá ser fornecida a qualquer cidadão identificado que a solicitar, em formato aberto, independente de motivação, exceto aquela que se inclua no disposto no art. 26 desta Resolução.

Art. 32. Será passível de classificação qualquer informação que provoque riscos à vida, segurança ou saúde da população, ou riscos à defesa, economia ou relações internacionais do Estado, e aquela que, no âmbito do TJPI, provoque assimetria competitiva ou privilégio entre agentes regulados, exponha o TJPI a ataques ou fraudes, ou que pertença a normas, autorizações, estudos e fiscalizações que componham processo não concluído.

Seção VII

Da gestão de riscos e da gestão de incidentes

Art. 33. O processo de gestão de riscos de segurança da informação alinha-se à gestão de riscos da segurança institucional.

Art. 34. A gestão de incidentes em segurança da informação tem por objetivo assegurar que fragilidades e incidentes em segurança da informação sejam identificados, para permitir a tomada de ação corretiva em tempo hábil.

Parágrafo único. Autoridades, servidores e quaisquer colaboradores do Tribunal são responsáveis por:

I - informar imediatamente à STIC os incidentes com a segurança da informação de que tenham ciência ou suspeita;

II - colaborar, na respectiva área de competência, com a identificação e o tratamento de incidentes em segurança da informação.

Seção VIII

Da segurança em Tecnologia da Informação e Comunicações - TIC

Art. 35. Compete à Secretaria de Tecnologia da Informação e Comunicações - STIC planejar, estabelecer em regulamentos específicos, monitorar e revisar periodicamente os procedimentos acerca do uso de recursos de Tecnologia da Informação - TI, controle de acesso, política de e-mail, política de uso da internet, política de uso de antivírus, política de acesso remoto e política de acesso a serviços de TI por fornecedores.

§ 1º Os ativos de TIC serão geridos pela STIC e acondicionados em local adequado ficando vedada a destinação não autorizada dos mesmos.

§ 2º Os ativos de TIC quando descartados serão tratados para que não levem consigo ativos de informação.

Art. 36. A certificação digital no âmbito do TJPI segue o padrão da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, instituída pela Medida Provisória 2.200-2, de 24 de agosto de 2001.

Art. 37. A assinatura digital de documentos deve ser realizada preferencialmente por meio de certificado digital, sendo permitida a utilização de usuário (login) e senha fornecidos mediante procedimento de cadastro no qual esteja assegurada a adequada identificação presencial ou remota do interessado.

§ 1º O procedimento de cadastro tratado no caput deste artigo deverá ser regulamentado em ato normativo próprio, devendo envolver, no mínimo:

I - endereço eletrônico para realização de pré-cadastro do interessado;

II - endereço da unidade responsável pela validação presencial dos documentos exigidos;

III - informações sobre procedimentos para alteração e redefinição de senha de acesso, em caso de perda;

IV - informações sobre a responsabilidade do usuário quanto a guarda e sigilo da senha de acesso;

V - informações sobre regras de cancelamento e bloqueio dos usuários.

§ 2º O cadastro de magistrados e servidores mantido pela Secretaria de Administração e Pessoas - SEAD, poderá ser utilizado para simplificar o procedimento de cadastro referido no caput deste artigo, substituindo a necessidade de nova identificação presencial dos usuários.

TÍTULO III

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 38. Ato do Presidente do TJPI deve instituir e regulamentar órgão colegiado de Segurança Institucional de natureza consultiva e deliberativa, de caráter permanente, que tem por finalidade:

I - formular e conduzir diretrizes para o Sistema de Gestão de Segurança da Informação - SGSI e para a Política de Segurança da Informação - PSI, bem como analisar periodicamente sua efetividade;

II - propor ajustes no SGSI e nas ações necessárias a sua implementação, com subsídio no monitoramento e na avaliação periódica das práticas de segurança da informação;

III – propor a elaboração e a revisão de normas e de procedimentos sobre os temas segurança da informação, transparência, acesso à informação e proteção de dados pessoais;

IV - manifestar-se sobre propostas de alteração ou de revisão da PSI, bem como sobre minutas de ato normativo e iniciativas de natureza estratégica ou que necessitem de cooperação entre unidades, que versem sobre segurança da informação;

V - manifestar-se sobre matérias atinentes à segurança da informação que lhe sejam submetidas;

VI - assessorar, em matérias correlatas, a Presidência do TJPI.

§ 1º O exame pelo CGSI de aspectos que perpassem as demais dimensões da segurança institucional deve ser realizado em reunião conjunta com o Gabinete de Segurança do TJPI, da qual emane

deliberação única de ambas as áreas.

Parágrafo único. O exame pelo órgão colegiado referido no caput deste artigo de aspectos que perpassem as demais dimensões da segurança institucional deve ser realizado em reunião conjunta com o Gabinete de Segurança Institucional, da qual emane deliberação única de ambas as áreas.

Art. 39. Compete ao Comitê de Gestão de TIC:

I - gerenciar e monitorar o SGSI, bem como propor as adaptações necessárias para garantir a melhoria contínua desse sistema de gestão;

II - coordenar e acompanhar a implementação do SGSI e das normas complementares de segurança da informação;

III - apresentar ao CGSI proposta de revisão da PSI de modo a atualizá-la diante de novos requisitos corporativos;

IV - apoiar as unidades do TJPI na definição de processos de trabalho e de procedimentos operacionais necessários à proteção de suas informações;

V - monitorar e avaliar periodicamente as práticas de segurança da informação adotadas pelo Tribunal;

VI - coordenar, com o apoio da Escola da Judiciária - EJUD do TJPI e das demais unidades competentes, ações permanentes de divulgação, treinamento, educação e conscientização dos servidores e demais colaboradores do TJPI, em relação aos conceitos e às práticas de segurança da informação em toda sua abrangência;

VII - coordenar o tratamento dos incidentes com segurança da informação, com vistas a identificar os motivos que levam ao comprometimento da segurança da informação; e

VIII - assessorar tecnicamente o CGSI.

Parágrafo único. A aplicação das competências indicadas neste artigo observa, no que couber, as competências inerentes às demais unidades da Secretaria de TIC do TJPI.

Art. 40. São responsabilidades do gestor da informação, no que concerne às informações sob sua gestão produzidas ou custodiadas pelo TJPI:

I - garantir a segurança das informações;

II - classificar as informações e definir procedimentos e critérios de acesso, observados os dispositivos legais e regimentais relativos à confidencialidade e a outros critérios de classificação pertinentes;

III - propor regras específicas para o uso das informações;

IV - definir os requisitos de segurança da informação necessários ao negócio, com base em critérios de aceitação e tratamento de riscos inerentes aos processos de trabalho.

§ 1º Presidente, Desembargadores e Juízes podem indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação.

§ 2º Em caso de dúvida na identificação do gestor da informação, compete à CGSI defini-lo.

Art. 41. É responsabilidade do custodiante da informação:

I - garantir a segurança da informação sob sua posse, conforme os critérios definidos pelo respectivo gestor da informação;

II - comunicar tempestivamente ao gestor da informação sobre situações que comprometam a segurança das informações sob custódia;

III - comunicar ao gestor da informação eventuais limitações para o cumprimento dos critérios por ele definidos com vistas à proteção da informação.

Art. 42. É responsabilidade dos dirigentes das unidades e demais gestores do TJPI, no que se refere à segurança da informação:

I - conscientizar servidores e quaisquer colaboradores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

III - tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas em tempo hábil, em caso de comprometimento da segurança da informação.

TÍTULO IV
DAS PENALIDADES

Art. 43. O não cumprimento das determinações da PSI sujeita o infrator às penalidades previstas na legislação e nos regulamentos internos do TJPI.

Art. 44. O descumprimento das disposições constantes nessa Política e nas normas complementares sobre segurança da informação caracteriza infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e civil.

Art. 45. O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei Complementar Nº 13 de 03/01/1994 e na legislação pertinente.

Art. 46. Os casos não previstos e as dúvidas surgidas na aplicação dessa Política serão submetidos ao CGSI.

TÍTULO V
DA ATUALIZAÇÃO

Art. 47. A PSI deve ser revisada e atualizada anualmente, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

TÍTULO VI
DISPOSIÇÕES FINAIS

Art. 48. Todos os procedimentos referentes à PSI adotados pelas unidades do TJPI deverão ser publicados para conhecimento geral.

Art. 49. Os contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo Tribunal devem observar, no que couber, as disposições desta Resolução.

Art. 50. Os atos necessários para regulamentar esta Resolução serão expedidos pelo Presidente do TJPI.

Art. 51. Esta Resolução entra em vigor na data de sua publicação.

Art. 52. Fica revogada a Resolução Nº 026/2009, de 16 de julho de 2009.

SALA VIRTUAL DAS SESSÕES DO EGRÉGIO TRIBUNAL PLENO, em Teresina (PI), 05 de julho de 2021.

Desembargador ***JOSÉ RIBAMAR OLIVEIRA***

PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO PIAUÍ

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Documento assinado eletronicamente por **José Ribamar Oliveira**, **Presidente**, em 07/07/2021, às 14:24, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **2535781** e o código CRC **D30573D4**.

Digite aqui o conteúdo do(s) anexo(s) ....

21.0.000052953-0 2535781v4