Referendada por unanimidade na 12ª SESSÃO ADMINISTRATIVA EXTRAORDINÁRIA DO ÓRGÃO ESPECIAL DO DIA 28 DE JUNHO DE 2023.
RESOLUÇÃO-GP Nº 39, DE 12 DE JUNHO DE 2023.

Código de validação: 0F38C3C539
RESOL-GP - 392023
(relativo ao Processo 255532023)

Dispõe sobre a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Maranhão.
O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a Lei nº 6.107, de 27 de julho de 1994, que dispõe sobre o Estatuto dos Servidores Públicos Civis do Estado, e dá outras providências;
CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, e dá outras providências;
CONSIDERANDO a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil;
CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018- Lei Geral de Proteção de Dados (LGPD);
CONSIDERANDO os termos da Resolução nº 363, de 12 de janeiro de 2021, do Conselho Nacional de Justiça - CNJ, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais;
CONSIDERANDO os termos da Resolução nº 370, de 28 de janeiro de 2021, do Conselho Nacional de Justiça - CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a Resolução nº 396, de 7 de junho de 2021, do Conselho Nacional de Justiça - CNJ, que Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Instrução Normativa nº 51, de 4 de julho de 2013, do Conselho Nacional de Justiça - CNJ, que dispõe sobre o uso dos recursos de tecnologia da informação e comunicação do Conselho Nacional de Justiça e dá outras providências;
CONSIDERANDO os Regimentos Internos do Tribunal de Justiçae da Corregedoria Geral da Justiçado Estado do Maranhão;
CONSIDERANDO a Resolução nº 50, de 19 de outubro de 2010, do Tribunal de Justiça do Estado do Maranhão - TJMA, que aprova o Regulamento Disciplinar dos Servidores do Poder Judiciário do Estado do Maranhão;
CONSIDERANDO a adoção de boas práticas relacionadas à gestão da informação, preconizadas pelas normas NBR ISO/IEC 27001, 27002, 27003, 27004 e 27005, que estabelecem objetivos, princípios e diretrizes para iniciar, implementar, manter, melhorar e auditar a segurança da informação em organizações de qualquer natureza;
CONSIDERANDO a necessidade de estabelecer políticas, normas e procedimentos de segurança da informação, com vistas a garantir a integridade, a disponibilidade, a confidencialidade, a autenticidade e a legalidade dos dados e informações;
CONSIDERANDO a importância dos ativos e/ou recursos de Tecnologia da Informação e Comunicação (TIC) e a necessidade de regular o uso da rede de dados corporativa do Poder Judiciário do Estado do Maranhão.
RESOLVE:
TÍTULO I
DISPOSIÇÕES GERAIS
Art. 1º Regulamentar a Política de Segurança da Informação (PSI) no âmbito do Poder Judiciário do Estado do Maranhão (PJMA), composta por normas e procedimentos complementares editados por este Tribunal de Justiça.
CAPÍTULO I
DAS DEFINIÇÕES
Art. 2º Para efeito desta Resolução, o termo usuário(a) refere-se a magistrado(a), servidor(a) efetivo(a) ou requisitado(a) e ocupante de cargo em comissão sem vínculo efetivo do Poder Judiciário do Estado do Maranhão.
Parágrafo único. Prestador(a) de serviço, colaborador(a), terceirizado(a), agente público(a) externo(a) e estagiário(a) será considerado(a) usuário(a), em caráter temporário, se for previamente autorizado(a) por procedimento formal, pela Diretoria de Informática e Automação(DIA), levando em consideração quaisquer responsabilidades legais durante a concessão de acesso.
Art. 3º Para fins desta Resolução, normas e procedimentos complementares, aplica-se a lista de termos do Glossário com suas respectivas definições, conforme descrito no Anexo I.
CAPÍTULO II
DOS PRINCÍPIOS E OBJETIVOS
Art. 4º A segurança da informação no Poder Judiciário do Estado do Maranhão alinha-se às estratégias organizacionais e aos seguintes princípios:
I - segurança e defesa cibernética;
II - segurança física das infraestruturas críticas;
III - segurança da informação confidencial;
IV - proteção contra vazamento de dados pessoais e institucionais;
V - ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade de dados e de informações;
VI - ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade das atividades administrativas, funcionais e/ou judiciais (atividades laborais);
VII - proteção dos dados organizacionais, dos ativos e dos recursos de Tecnologia da Informação e Comunicação (TIC) de forma geral;
VIII - responsabilização dos(as) usuários(as) pelos atos que comprometam a segurança dos ativos e/ou recursos de TIC;
IX - ações de planejamento, de sistematização e de normatização sobre temas atinentes à segurança cibernética;
X - ações de comunicação, de conscientização, de formação de cultura e de direcionamento institucional com vistas à segurança cibernética; e

XI - ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de Tecnologia da Informação e Comunicação (TIC).
Art. 5º A Política de Segurança da Informação do Poder Judiciário do Estado do Maranhão tem como objetivos:
I - tornar o PJMA mais seguro e inclusivo no ambiente digital;
II - instituir diretrizes gerais, princípios básicos, responsabilidades, competências e punições, visando à garantia da segurança da informação;
III - aumentar a resiliência do PJMA às ameaças cibernéticas;
IV - permitir a manutenção, a continuidade dos serviços ou o seu restabelecimento em menor tempo possível;
V - promover ações necessárias à implementação, gestão e manutenção da segurança da informação;
VI - estabelecer e fortalecer a governança, a gestão e a coordenação integrada de ações de segurança cibernética no PJMA; e
VII - combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos e/ou recursos de TIC, o sigilo e a imagem do PJMA.
CAPÍTULO III
DA ABRANGÊNCIA
Art. 6º A Política de Segurança da Informação se aplica a todos(as) usuários(as) que fazem uso dos ativos e/ou recursos de TIC do Poder Judiciário do Estado do Maranhão.
Art. 7º Os contratos, convênios, acordos de cooperação e outros instrumentos semelhantes celebrados pelo Poder Judiciário do Estado do Maranhão observarão, no que couber, o constante nesta Resolução, normas e procedimentos complementares.
CAPÍTULO IV
DA ESTRUTURA DE GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO
Seção I
Da Estrutura Normativa
Art. 8º A Política de Segurança da Informação(PSI)do Poder Judiciário do Estado do Maranhão(PJMA) está estruturada em três níveis hierárquicos, assim dispostos:
I - nível estratégico: compreende a Política de Segurança da Informação(PSI)deste ato, que norteia a criação de normas e procedimentos complementares e traça diretrizes base de segurança da informação;
II - nível tático: compreende as normas complementares, que derivam desta Resolução, especificando obrigações a serem seguidas pelos(as) usuários(as), regras e procedimentos em nível gerencial relacionadas à gestão dos ativos e/ou recursos de TIC de acordo com as diretrizes estabelecidas nesta PSI;
III - nível operacional: procedimentos de segurança da informação que contemplam regras operacionais, roteiros técnicos, fluxos de processos, manuais com informações técnicas que instrumentalizam o disposto na PSI e nas normas complementares referenciadas no nível tático.
Seção II
Da Aprovação e Revisão
Art. 9º A PSI será revisada e atualizada periodicamente, a cada 2(dois) anos, ou, caso ocorram eventos ou fatos relevantes que exijam uma revisão imediata, sendo submetida à apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI) e do Órgão Especial.
Art. 10. As normas complementares e procedimentos, que também fazem parte desta PSI, denominadas anexos, podem ser alteradas mediante necessidade de suas atualizações, com apreciação e aprovação por parte do Comitê de Governança de Segurança da Informação (CGSI).
CAPÍTULO V
DAS NORMAS
Art. 11. Serão criadas, revisadas e atualizadas, consoante o estabelecido no artigo 10 desta Resolução, normas complementares e procedimentos, sem prejuízo de normativos adicionais sobre outros temas e conforme necessidade e conveniência, para as seguintes seções:
I - controle de acesso e gestão de identidade;
II - classificação e tratamento da informação;
III - segurança física no ambiente de TIC;
IV - gestão de ativos;
V - uso aceitável de ativos;
VI - gestão de incidentes de segurança da informação;
VII - cópias de segurança da informação;
VIII - gestão de criptografia e gerenciamento de chaves;
IX - proteção contra códigos maliciosos;
X - gestão de vulnerabilidades técnicas;
XI - desenvolvimento seguro;
XII - proteção de dados pessoais;
XIII - registro de eventos;
XIV - gestão de riscos da segurança da informação;
XV - plano de gestão de continuidade de negócios; e
XVI - gestão de serviços em nuvem.
Parágrafo único. As normas complementares e os procedimentos previstos nesta Resolução deverão ser obedecidas por todos(as) os(as) usuários(as) do PJMA.
Seção I
Norma de controle de acesso e gestão de identidade
Art. 12. A norma de controle de acesso e gestão de identidade será regulamentada no Anexo II, com diretrizes específicas e procedimentos próprios, e observará os seguintes objetivos:
I - assegurar o acesso autorizado e mitigar o acesso não autorizado a informações, ativos e/ou recursos de TIC do PJMA;

II - permitir a identificação única de indivíduos que acessam informações, ativos e/ou recursos de TIC do PJMA com a cessão adequada dos direitos de acesso.

Seção II

Norma de classificação e tratamento da informação

Art. 13. A norma de classificação e tratamento da informação será regulamentada no Anexo III, com diretrizes específicas e procedimentos próprios, e atenderá ao seguinte objetivo:

I - garantir a identificação e o entendimento das necessidades de proteção das informações de acordo com a sua relevância para a organização.

Seção III

Norma de segurança física no ambiente de TIC

Art. 14. A norma de segurança física no ambiente de TIC será regulamentada no Anexo IV, com diretrizes específicas e procedimentos próprios, e contemplará o seguinte objetivo:

I - mitigar acesso físico não autorizado, danos e interferências nas informações, ativos e/ou recursos de TIC críticos do PJMA.

Seção IV

Norma de gestão de ativos

Art. 15. A norma de gestão de ativos será regulamentada no Anexo V, com diretrizes específicas e procedimentos próprios, e obedecerá ao seguinte objetivo:

I - identificar as informações, ativos e/ou recursos de TIC da organização, a fim de preservar a segurança da informação e atribuir propriedades adequadas.

Seção V

Norma de uso aceitável de ativos

Art. 16. A norma de uso aceitável de ativos será regulamentada no Anexo VI, com diretrizes específicas e procedimentos próprios, e seguirá os seguintes objetivos:

I - assegurar que as informações, ativos e/ou recursos de TIC da organização sejam devidamente protegidos, utilizados e/ou manuseados;

II - reduzir os riscos de acessos não autorizados, perdas e danos às informações em mesas, telas e em outros locais acessíveis durante e fora do horário de expediente;

III - manter a segurança das informações transferidas dentro da organização e com qualquer parte externa interessada;

IV - elaborar requisitos específicos de segurança cibernética relativos aos ativos de TIC sob sua jurisdição, incluindo ambientes centralizados, endpoints, equipamentos intermediários ou finais conectados em rede ou a algum sistema de comunicação, inclusive equipamentos portáteis e dispositivos móveis;

V - elaborar requisitos específicos de segurança cibernética relacionados com o acesso remoto;

VI - certificar a utilização adequada dos recursos de TIC, no que se refere ao uso do correio eletrônico, dos sistemas de informação, da *internet* e do ambiente colaborativo (armazenamento remoto, agenda/calendário, videoconferência, bate-papo e suíte de escritório);

VII - garantir a inserção, divulgação, modificação, manutenção ou remoção de informações apenas de forma autorizada sobre as mídias de armazenamento.

Seção VI

Norma de gestão de incidentes de segurança da informação

Art. 17. A norma de gestão de incidentes de segurança da informação será regulamentada no Anexo VII, com diretrizes específicas e procedimentos próprios, a qual apreciará os seguintes objetivos:

I - assegurar uma resposta rápida, eficiente, eficaz e ordenada aos incidentes de segurança da informação, incluindo a comunicação interna e externa sobre os eventos ocorridos e procedimento de continuidade do serviço prestado;

II - assegurar a efetiva categorização e priorização de eventos de segurança da informação;

III - reduzir a probabilidade ou as consequências de incidentes;

IV - assegurar uma gestão consistente e eficaz das evidências relacionadas a incidentes de segurança da informação para fins de ações disciplinares e legais;

V - realizar práticas e simulações de incidentes para efetivar o aprimoramento contínuo do processo de gestão de incidentes;

VI - utilizar tecnologia que favoreça o conhecimento de ameaças cibernéticas em redes de informação, especialmente em fóruns e comunidades virtuais, inclusive de iniciativa privada; e

VII - estabelecer troca de informações e boas práticas com outros membros do poder público em geral e do setor privado de forma colaborativa.

Seção VII

Norma de cópias de segurança da informação

Art. 18. A norma de cópias de segurança da informação será regulamentada no Anexo VIII, com diretrizes específicas e procedimentos próprios, e observará os seguintes objetivos:

I - providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, de forma que permita a investigação de incidentes;

II - realizar a guarda, preservação ou eliminação de cópias de segurança seguindo tempo de retenção estabelecido;

III - possibilitar a recuperação da perda de dados ou sistemas através das cópias de segurança realizadas;

IV - realizar testes de recuperação a fim de garantir a efetividade da realização das cópias de segurança.

Seção VIII

Norma de gestão de criptografia e gerenciamento de chaves

Art. 19. A norma de gestão de criptografia e gerenciamento de chaves será regulamentada no Anexo IX, com diretrizes específicas e procedimentos próprios, e atenderá o seguinte objetivo:

I - assegurar o uso adequado e eficaz da criptografia para proteger a confidencialidade, autenticidade e integridade das informações de acordo com os requisitos de segurança da informação da organização, levando em consideração os requisitos legais, estatutários, regulamentares e contratuais relacionados à criptografia.

Seção IX

Norma de proteção contra códigos maliciosos

Art. 20. A norma de proteção contra códigos maliciosos será regulamentada no Anexo X, com diretrizes específicas e procedimentos próprios, e contemplará o seguinte objetivo:

I - assegurar que informações, ativos de TIC e recursos de processamento da informação estejam protegidos contra códigos maliciosos.

Seção X

Norma de gestão de vulnerabilidades técnicas

Art. 21. A norma de gestão de vulnerabilidades técnicas será regulamentada no Anexo XI, com diretrizes específicas e procedimentos próprios, e observará o seguinte objetivo:

I - assegurar a integridade dos sistemas operacionais e mitigar a exploração de vulnerabilidades técnicas conhecidas.

Seção XI

Norma de desenvolvimento seguro

Art. 22. A norma de desenvolvimento seguro será regulamentada no Anexo XII, com diretrizes específicas e procedimentos próprios, e obedecerá os seguintes objetivos:

I - garantir que a segurança da informação seja implementada em todo ciclo de vida de desenvolvimento dos sistemas de informação;

II - atender aos princípios e requisitos de segurança da informação para sistemas de informação adquiridos pelo TJMA;

III - atender aos princípios e requisitos de segurança da informação para sistemas de informação mantidos e/ou desenvolvidos pela equipe de sistemas do TJMA ou por terceirizados e/ou contratados supervisionados pela equipe de sistemas do TJMA;

IV - adotar práticas e requisitos de segurança cibernética no desenvolvimento de projetos novos ou em desenvolvimento, tais como ativação do Múltiplo Fator de Autenticação (MFA).

Seção XII

Norma de proteção de dados pessoais

Art. 23. A norma de proteção de dados pessoais será regulamentada no Anexo XIII, com diretrizes específicas e procedimentos próprios, e cumprirá o seguinte objetivo:

I - assegurar o cumprimento dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação da proteção de dados pessoais.

Seção XIII

Norma de registro de eventos

Art. 24. A norma de registro de eventos será regulamentada no Anexo XIV, com diretrizes específicas e procedimentos próprios, e apreciará os seguintes objetivos:

I - registrar eventos, gerar evidências, assegurar a integridade das informações de registro, prevenir contra acesso não autorizado, identificar eventos de segurança da informação que possam levar a um incidente de segurança e apoiar investigações;

II - utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de TIC e de ações dos(as) usuários(as), permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.

Seção XIV

Norma de gestão de riscos

Art. 25. A norma de gestão de riscos será regulamentada no Anexo XV, com diretrizes específicas e procedimentos próprios, e observará os seguintes objetivos:

I - contextualizar e identificar os riscos;

II - analisar e estabelecer ordem prioritária dos riscos;

III - avaliar e priorizar as ações para reduzir a ocorrência dos riscos;

IV - tratar periodicamente os riscos;

V - monitorar os riscos;

VI - comunicar os riscos aos responsáveis;

VII - envolver as partes interessadas nas decisões de gestão de riscos; e

VIII - coletar informações de forma a melhorar a abordagem da gestão de riscos.

Seção XV

Plano de gestão de continuidade de negócios

Art. 26. O plano de gestão de continuidade dos negócios será regulamentado no Anexo XVI, com diretrizes específicas e procedimentos próprios, e atenderá o seguinte objetivo:

I - planejar, implementar, manter e testar a prontidão do plano baseado nos objetivos e requisitos de continuidade de negócios.

Seção XVI

Norma de gestão de serviços em nuvem

Art. 27. A norma de gestão de serviços em nuvem será regulamentada no Anexo XVII, com diretrizes específicas e procedimentos próprios, e observará o seguinte objetivo:

I - especificar e gerenciar a segurança da informação para o uso de serviços em nuvem.

CAPÍTULO VI

CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

Art. 28. A conscientização e treinamento em segurança da informação seguirá as seguintes diretrizes gerais:

I - o programa de conscientização em segurança da informação deverá tornar os(as) usuários(as) conscientes de suas responsabilidades;

II - o programa de conscientização estará alinhado às normas e procedimentos relevantes de segurança da informação;

III - as atividades do programa de conscientização em segurança da informação serão realizadas periodicamente;

IV - os programas de conscientização sobre segurança da informação serão implementados através de treinamentos específicos.

Art. 29. Os treinamentos disponibilizados serão compatíveis com as tecnologias atualmente implementadas no ambiente informatizado.
Art. 30. As diretrizes básicas da PSI e das normas deverão ser divulgadas em todas as unidades do PJMA, garantindo que todos(as) tomem ciência delas e as pratiquem.
TÍTULO II
DOS PAPÉIS E RESPONSABILIDADES
CAPÍTULO I
DOS GESTORES DAS UNIDADES JUDICIAIS OU ADMINISTRATIVAS
Art. 31. É responsabilidade dos gestores das unidades judiciais ou administrativas:
I - conhecer, divulgar, cumprir e estimular o cumprimento da PSI e suas normas complementares, promovendo a adequada utilização dos ativos e/ou recursos de TIC, zelando pelos princípios da segurança da informação;
II - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;
III - assegurar a observância da PSI no âmbito de sua unidade, bem como comunicar, de imediato, à DIA qualquer irregularidade constatada, para as providências legais cabíveis;
IV - solicitar formalmente à DIA a concessão de permissões de acesso aos(às) usuários(as) sob sua supervisão, sempre com base no binômio "necessidade e mínimo de permissões", para executar atividades administrativas, funcionais e/ou judiciais;
V - comunicar formalmente à Diretoria de Recursos Humanos qualquer ocorrência de mudança de lotação, afastamento, retorno ou desligamento de usuários(as);
VI - manter o zelo e bom uso, em nível físico e lógico, dos ativos e/ou recursos de TIC sob responsabilidade de sua unidade de atuação;
VII - tomar medidas administrativas cabíveis para que sejam adotadas ações corretivas, no caso de descumprimento da Política de Segurança da Informação.
CAPÍTULO II
DAS UNIDADES JUDICIAIS E ADMINISTRATIVAS
Seção I
Da Diretoria de Informática e Automação
Art. 32. A Diretoria de Informática e Automação (DIA) é a unidade responsável pela normatização da Política de Segurança da Informação no Poder Judiciário do Estado Maranhão, competindo-lhe aplicar, no âmbito de suas responsabilidades, a própria PSI, as normas e procedimentos complementares, garantindo os princípios da segurança da informação;
Parágrafo único. Compete aos(às) servidores(as) lotados(as) na Diretoria de Informática e Automação a gestão do ambiente computacional, bem como o acesso com perfil de administrador aos ativos e/ou recursos de TIC do PJMA.
Art. 33. Compete à Diretoria de Informática e Automação:
I - garantir os princípios de segurança da informação aos ativos e/ou recursos de TIC da rede de dados corporativa do PJMA;
II - disponibilizar aos(às) usuários(as): acesso remoto, áreas de armazenamento de arquivos, acesso à *internet*, serviço de correio eletrônico, serviço de ambiente colaborativo, sistemas de informação, ativos e recursos de TIC do PJMA para execução de suas atividades laborais;
III - gerir e manter o acesso remoto, as áreas de armazenamento de arquivos, o acesso à *internet*, o serviço de correio eletrônico, o serviço de ambiente colaborativo, os sistemas de informação, e demais ativos e recursos de TIC do PJMA;
IV - realizar auditorias de acessos dos(as) usuários(as) periodicamente ou quando solicitado pela administração, pelo(a) superior imediato(a) ou pelo(a) próprio(a) usuário(a);
V - aplicar controles para monitorar e gerir acesso às informações consideradas inadequadas ou não relacionadas às atividades laborais, especialmente sítios eletrônicos de conteúdo agressivo, homofóbico, terrorista, de cunho racista, de uso de drogas ilícitas, de aborto, de pornografia, assim como qualquer outro que possa infringir a legislação vigente; de entretenimento, de jogos, de redes sociais, de mensagens instantâneas e com conteúdos que incentivam a pirataria, bem como restringir o acesso a serviços que podem tornar os ativos e/ou recursos de TIC vulneráveis a invasões externas e ataques, em suas mais diferentes formas, levando à perda dos princípios da segurança da informação;
VI - identificar o uso inadequado dos ativos e/ou recursos de TIC e adotar as medidas apropriadas; e
VII - elaborar e coordenar as campanhas de conscientização sobre segurança da informação.
Seção II
Da Diretoria de Recursos Humanos
Art. 34. É responsabilidade da Diretoria de Recursos Humanos:
I - manter atualizadas as informações do sistema de recursos humanos, priorizando aquelas que se referem a nomeação, afastamento, mudança de lotação, retorno, desligamento, aposentadoria, falecimento ou qualquer outra mudança no quadro funcional do Poder Judiciário do Estado do Maranhão e órgãos subordinados;
II - apoiar as campanhas de conscientização de segurança da informação;
III - elaborar e instituir o Termo de Responsabilidade e Confidencialidade como documento obrigatório para o exercício dos cargos e funções;
IV - adotar as medidas necessárias por ocasião do desligamento do(a) servidor(a) e comunicar imediatamente e formalmente a DIA e demais setores interessados para revogação dos acessos e permissões do(a) usuário(a) aos ativos e/ou recursos de TIC do PJMA;
V - comunicar à DIA qualquer ocorrência de nomeação de servidor(a) para o devido credenciamento do(a) usuário(a) para acessar os ativos e/ou recursos de TIC do PJMA ou de nomeação de cargo ou função para redefinição das permissões de sua credencial de acesso;
VI - notificar à DIA ocorrências de afastamento, mudança de lotação, retorno, desligamento, exoneração de cargo ou função, aposentadoria e/ou falecimento de servidor(a) para redefinição das permissões de sua credencial de acesso.
Seção III
Da Assessoria de Comunicação
Art. 35. Compete à Assessoria de Comunicação:

I - promover e divulgar campanhas de conscientização de segurança da informação.

Seção IV

Da Assessoria Jurídica da Presidência

Art. 36. Compete à Assessoria Jurídica da Presidência do Poder Judiciário do Estado do Maranhão:

I - avaliar, sempre que solicitada, a Política de Segurança da Informação, as normas, os procedimentos complementares e o Termo de Responsabilidade e Confidencialidade referentes à gestão da segurança da informação;

II - informar ao Comitê de Governança de Segurança da Informação alterações legais ou regulatórias que impliquem responsabilidade ou ação que envolvam a gestão da segurança da informação;

III - auxiliar o CGSI nas demais questões legais.

Seção V

Da Diretoria de Segurança Institucional e Gabinete Militar

Art. 37. Compete à Diretoria de Segurança Institucional e Gabinete Militar do Poder Judiciário do Estado do Maranhão:

I - apoiar a aplicação da norma de segurança física e do ambiente;

II - proibir o acesso físico de pessoas não autorizadas ao PJMA que possam vir a causar danos e interferências nas informações, nos ativos e/ou recursos de TIC do PJMA;

III - controlar o acesso físico e a permanência de pessoas autorizadas ao PJMA, de acordo com seus níveis de permissão, por meio de sistemas de identificação biométrica, sempre que a tecnologia estiver disponível.

Seção VI

Da Diretoria de Auditoria Interna

Art. 38. Compete à Diretoria de Auditoria Interna do Poder Judiciário do Estado do Maranhão:

I - realizar, a cada 2(dois) anos, avaliação para aferir o cumprimento dos controles e procedimentos estabelecidos nesta Resolução.

Seção VII

Da Presidência

Art. 39. Compete à Presidência do Poder Judiciário do Estado do Maranhão:

I - apoiar a aplicação das ações estabelecidas nesta PSI, das normas complementares e procedimentos.

Seção VIII

Da Escola Superior da Magistratura do Estado do Maranhão - ESMAM

Art. 40. Compete à Escola Superior da Magistratura do Estado do Maranhão:

I - promover cursos de capacitação e conscientização sobre segurança da informação para os(as) usuários(as) do PJMA conforme calendário definido com apoio da DIA.

TÍTULO III

UTILIZAÇÃO DOS ATIVOS E RECURSOS DE TIC

Art. 41. Todas as informações geradas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas pelo(a) usuário(a) no desempenho de suas atividades laborais são de propriedade e/ou de direito de uso exclusivo do PJMA.

Art. 42. O uso adequado dos ativos e/ou recursos de TIC pelos(as) usuários(as) visa garantir a continuidade da prestação jurisdicional e administrativa do Poder Judiciário do Estado do Maranhão.

§ 1º A utilização dos ativos e/ou recursos de TIC pelos(as) usuários(as) é pautada pelos princípios da celeridade, ética, segurança, responsabilidade e legalidade.

§ 2º O(A) usuário(a) deverá ainda garantir a disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e auditabilidade das informações produzidas, recebidas, armazenadas, tratadas e transmitidas relacionadas em suas atividades administrativas, funcionais e/ou judiciais.

Art. 43. Os ativos e/ou recursos de TIC disponíveis para os(as) usuários(as), pertencentes ao PJMA, serão utilizados para desenvolvimento de atividades laborais, fazendo uso de suas credenciais de acesso, exclusivamente.

Parágrafo único. As credenciais de acesso são pessoais e intransferíveis; toda e qualquer ação executada pelo(a) usuário(a) utilizando uma determinada credencial será de responsabilidade exclusiva do(a) mesmo(a), devendo este(a) zelar por sua confidencialidade.

Art. 44. Os ativos e/ou recursos de TIC de propriedade do PJMA deverão ser utilizados apenas por usuários(as) autorizados(as), conforme descrito no artigo 2º.

Art. 45. A utilização dos ativos e/ou recursos de TIC é passível de monitoramento e controle por parte do Poder Judiciário do Estado do Maranhão, respeitando, em todo caso, os preceitos das legislações vigentes.

Art. 46. É dever de todos(as) os(as) usuários(as) dos ativos e/ou recursos de TIC do Poder Judiciário do Estado do Maranhão:

I - conhecer, compreender e cumprir esta Política de Segurança da Informação, bem como suas normas e procedimentos complementares, aplicáveis às suas atividades;

II - firmar, obrigatoriamente, Termo de Responsabilidade e Confidencialidade sobre as informações relacionadas às suas atividades;

III - alertar a DIA sobre violações desta PSI e/ou das normas em anexo;

IV - proteger as informações confidenciais e pessoais obtidas em decorrência do exercício de suas atividades laborais;

V - preservar o sigilo da identificação de usuário(a) e de senhas de acessos individuais a sistemas de informação ou de outros tipos de credenciais de acesso que lhes forem atribuídas;

VI - participar das campanhas de conscientização e dos treinamentos pertinentes aos temas segurança da informação e proteção de dados pessoais, conforme planejamento do PJMA;

VII - utilizar os ativos e/ou recursos de TIC sob sua responsabilidade de forma segura, em observância ao disposto nesta PSI e nas normas e procedimentos complementares;

VIII - proteger os ativos e/ou recursos de TIC contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizadas;

IX - não divulgar, compartilhar e/ou transmitir informações confidenciais de trabalho em ambientes públicos;

X - não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente externo, sem

controle ou sem autorização formal do PJMA;
XI - atentar ao repassar e/ou transmitir informações para outras pessoas, seja de forma presencial, via telefone ou dispositivos móveis, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais, confirmando a identidade e idoneidade do solicitante ou destinatário antes dos seus envios;
XII - reportar tempestivamente ao proprietário da informação sobre situações que comprometam a segurança das informações sob sua custódia;
XIII - comunicar à Diretoria de Informática e Automação controles inadequados que restrinjam acesso a conteúdos relacionados às atividades administrativas, funcionais e/ou judiciais, para providências cabíveis;
XIV - comunicar ao proprietário da informação eventuais limitações para o cumprimento dos critérios por ele definidos com vistas à proteção da informação; e
XV - não divulgar, compartilhar, transmitir, veicular ou permitir a divulgação, por qualquer meio, informações sobre ativos e/ou recursos de TIC ou de procedimentos do PJMA, exceto quando houver autorização prévia e formal de superior hierárquico(a) ou de acordo com legislação vigente para tal.
Art. 47. Compete ao(a) usuário(a) garantir a confidencialidade, integridade e disponibilidade das informações produzidas e armazenadas nos ativos e/ou recursos de TIC utilizados dentro e fora do ambiente da rede de dados corporativa do PJMA.
Art. 48. Os(As) usuários(as) deverão reportar incidentes que afetam a segurança dos ativos e/ou recursos de TIC.

TÍTULO IV

DAS INFRAÇÕES E DAS PENALIDADES

Art. 49. É considerado descumprimento da PSI pelo(a) usuário(a):
I - fornecer, por qualquer motivo, sua credencial de acesso para outrem;
II - usar a credencial de outrem para acesso ou utilização de ativos e/ou recursos de TIC;
III - obter acesso não autorizado a qualquer computador, rede, banco de dados, sistemas de informação ou informações guardadas eletronicamente;
IV - divulgar informações de uso restrito ou confidenciais, assim definidas em lei ou regulamento próprio, contidas nos sistemas de informações ou bancos de dados do Judiciário;
V - inserir ou facilitar a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas de informação ou bancos de dados do Judiciário, a fim de obter vantagem indevida para si ou para outrem ou para causar danos;
VI - utilizar os ativos e/ou recursos de TIC para transferência e armazenamento de arquivos que não estejam relacionados às atividades administrativas, funcionais e/ou judiciais, incluindo arquivos de *software*, documentos, imagens, áudio e vídeo;
VII - usar os ativos e/ou recursos de TIC para armazenamento, distribuição, divulgação, manipulação, cópia, transmissão, disponibilização ou publicação de conteúdos que contenham teor sexual, ofensivo, preconceituoso, discriminatório, terrorista, subversivo, injurioso, calunioso, difamatório, vexatório ou agressivo à dignidade humana;
VIII - utilizar os ativos e/ou recursos de TIC para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos e normativos internos do PJMA;
IX - instalar e/ou configurar ativos de TIC sem o acompanhamento, a homologação, ciência ou autorização da Diretoria de Informática e Automação;
X - fazer uso de qualquer tipo de ativo e/ou recurso de TIC não contratado, licenciado ou homologado pela DIA;
XI - utilizar os ativos e/ou recursos de TIC de forma a interferir no trabalho dos(as) demais usuários(as) ou que comprometa o desempenho e/ou a segurança das informações existentes na rede de dados corporativa do PJMA.
Art. 50. O descumprimento das disposições desta Resolução, normas complementares, procedimentos ou qualquer outra prática e/ou conduta não autorizada expressamente pela DIA, que cause dano aos ativos e/ou recursos de TIC do PJMA, poderá submeter o(a) usuário(a) às penalidades previstas na legislação e nos regulamentos internos do TJMA, podendo ser apuradas em Processo Administrativo Disciplinar, assegurado o contraditório e a ampla defesa, sem prejuízo das ações cíveis ou penais cabíveis.
§ 1º As infrações desta Resolução, bem como das demais normas complementares, mesmo que por mera omissão ou tentativa não consumada, serão passíveis de penalidades, tais como: advertência, repreensão, suspensão, demissão e destituição do cargo em comissão ou de função gratificada, podendo ser aplicadas isoladas ou cumulativamente.
§ 2º A execução de sanções e penalidades será realizada conforme análise do Comitê de Governança de Segurança da Informação do TJMA, podendo o CGSI, no uso de suas competências, aplicar ações corretivas e disciplinares cabíveis nos casos de violação da segurança da informação.
§ 3º No caso de prestador(a) de serviço, colaborador(a), terceirizado(a) e/ou estagiário(a) o CGSI deverá analisar o descumprimento e deliberar sobre a efetivação das sanções e penalidades conforme termos previstos nos contratos formalizados.
Art. 51. O(A) usuário(a) identificado(a) como infrator(a) de alguma das disposições desta Resolução poderá ter sua credencial de acesso bloqueada ou restringida, considerado o interesse da Administração, a partir da solicitação para instauração de Processo Administrativo Disciplinar, podendo o bloqueio ou restrição perdurar durante o trâmite da sindicância ou inquérito administrativo, sempre dando ciência ao(a) superior imediato(a).

TÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 52. A PSI e as normas complementares estarão disponibilizadas no sítio eletrônico mantido por este Tribunal de Justiça para conhecimento geral.
Art. 53. As exceções e os casos omissos serão submetidos ao Comitê de Governança de Segurança da Informação do Tribunal de Justiça do Estado do Maranhão para posterior deliberação.
Art. 54. Esta Resolução entrará em vigor na data de sua publicação, ficando revogada a Resolução GP nº 13, de 23 de março de 2017.
Dê-se ciência. Publique-se. Cumpra-se.

PALÁCIO DA JUSTIÇA "CLÓVIS BEVILÁCQUA" DO ESTADO DO MARANHÃO, em São Luís, 12 de junho de 2023.

Desembargador PAULO SÉRGIO VELTEN PEREIRA
Presidente do Tribunal de Justiça
Matrícula 126599

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 14/06/2023 15:17 (PAULO SÉRGIO VELTEN PEREIRA)

Informações de Publicação

Edição	Disponibilização	Publicação
107/2023	16/06/2023 às 15:18	19/06/2023

Informações de Publicação

60/2024	05/04/2024 às 16:48	08/04/2024